

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-232418**

(43)Date of publication of application : **16.08.2002**

(51)Int.Cl.

H04L 9/16

H04Q 7/38

(21)Application number : **2001-376564**

(71)Applicant : **LCENT TECHNOL INC**

(22)Date of filing : **11.12.2001**

(72)Inventor : **PATEL SARVAR**

(30)Priority

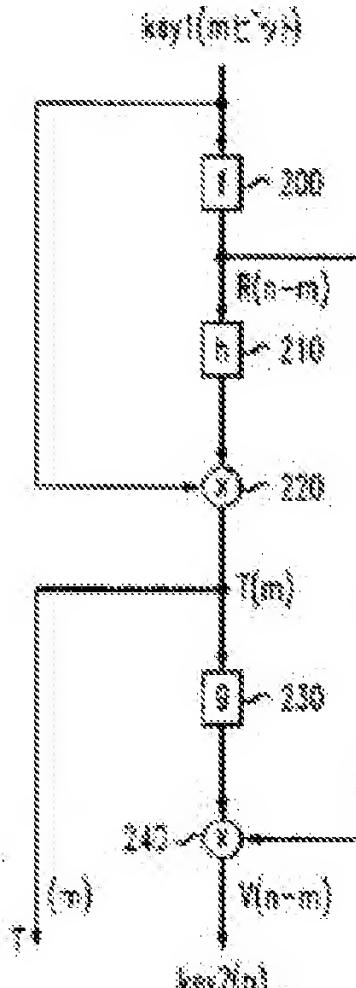
Priority number : **2000 734148** Priority date : **11.12.2000** Priority country : **US**

(54) SYSTEM AND METHOD FOR CONVERTING KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a key conversion system for deterministically and reversibly converting the first key value of a first communication system into the second key value of a second communication system.

SOLUTION: The key conversion system generates a first intermediate value from at least a portion of the first key value by using a first random function. At least a portion of the first intermediate value is provided to a second random function for producing a second value. Exclusive-OR(XOR) is performed on at least a portion of the first key value and at least a portion of the second value and a second intermediate value is generated. At least a portion of the second intermediate value is provided to a third random function for producing a third value. By performing exclusive-OR on at least a portion of the third value and at least a portion of the first intermediate value, the key conversion system produces at least the first portion of the second key value, and at least the second portion of the second key value is produced as the second intermediate value.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-232418
(P2002-232418A)

(43)公開日 平成14年8月16日 (2002.8.16)

(51)Int.Cl.⁷
H 04 L 9/16
H 04 Q 7/38

識別記号

F I
H 04 L 9/00
H 04 B 7/26

テマコート(参考)
6 4 3 5 J 1 0 4
1 0 9 S 5 K 0 6 7

審査請求 未請求 請求項の数10 O L (全 15 頁)

(21)出願番号 特願2001-376564(P2001-376564)
(22)出願日 平成13年12月11日 (2001.12.11)
(31)優先権主張番号 09/734148
(32)優先日 平成12年12月11日 (2000.12.11)
(33)優先権主張国 米国 (U.S.)

(71)出願人 596092698
ルーセント テクノロジーズ インコーポ
レーテッド
アメリカ合衆国 07974-0636 ニュージ
ャーシ, マレイ ヒル, マウンテン ア
ヴェニュー 600
(72)発明者 サーヴァー パテル
アメリカ合衆国 07045 ニュージャーシ
イ, モントヴィル, ミラー レーン 34
(74)代理人 100064447
弁理士 岡部 正夫 (外10名)

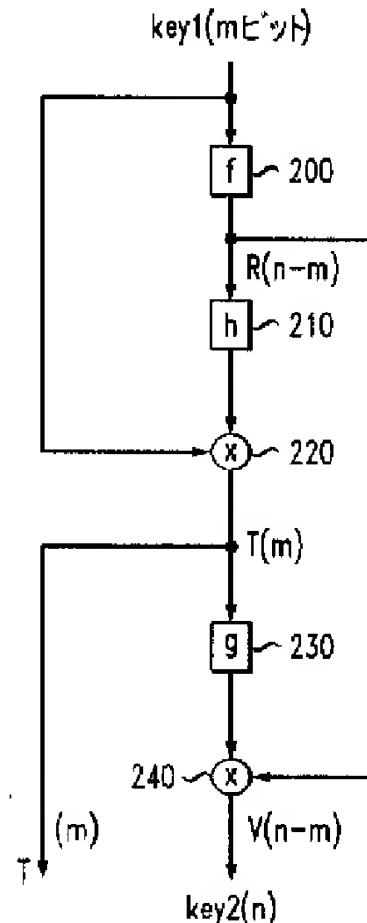
最終頁に続く

(54)【発明の名称】 鍵変換システムおよび方法

(57)【要約】

【課題】 本発明の目的は、第1の通信システムの第1の鍵値から第2の通信システムの第2の鍵値に、決定論的に、かつ可逆的に変換するための鍵変換システムを提供することである。

【解決手段】 鍵変換システムは、第1のランダム関数を用いて、第1の鍵値の少なくとも一部から第1の中間値を生成する。第1の中間値の少なくとも一部は、第2の値を生成するために第2のランダム関数に与えられる。第1の鍵値の少なくとも一部と、第2の値の少なくとも一部とにおいて排他的論理和 (XOR) が実行され、第2の中間値が生成される。第2の中間値の少なくとも一部は、第3の値を生成するために第3のランダム関数に与えられる。第3の値の少なくとも一部と、第1の中間値の少なくとも一部とにおいて排他的論理和を実行することにより、鍵変換システムは第2の鍵値の少なくとも第1の部分を生成し、第2の鍵値の少なくとも第2の部分は第2の中間値として生成される。



【特許請求の範囲】

【請求項1】 第1の通信システムのための第1の鍵値(KEY1)を第2の通信システムのための第2の鍵値(KEY2)に変換する方法であって、

第1のランダム関数(f)を用いて前記第1の鍵値(KEY1)の少なくとも一部から第1の中間値(R)を生成するステップと、

第2の値を生成するために、前記第1の中間値(R)の少なくとも一部を第2のランダム関数(h)に与えるステップと、

第2の中間値(T)を生成するために、前記第1の鍵値(KEY1)の少なくとも一部と、前記第2の値の少なくとも一部とについての排他的論理和(220)を実行するステップと、

第3の値を生成するために、前記第2の中間値(T)の少なくとも一部を第3のランダム関数(g)に与えるステップと、

前記第3の値の少なくとも一部と、前記第1の中間値(R)の少なくとも一部とについての排他的論理和(240)を実行することにより、前記第2の鍵値(KEY2)の少なくとも第1の部分を生成するステップとを含むことを特徴とする方法。

【請求項2】 前記第2の鍵値(KEY2)の少なくとも第2の部分として、前記第2の中間値(T)の少なくとも一部を生成することを特徴とする請求項1に記載の方法。

【請求項3】 前記第1の中間値(R)を生成する前記ステップは、

n-mビットの前記第1の中間値(R)を生成するためには、mビットの前記第1の鍵値(KEY1)を第1のランダム関数(f)に与えるステップを含むことを特徴とする請求項1に記載の方法。

【請求項4】 前記第1の中間値(R)の少なくとも一部を与える前記ステップと、排他的論理和を実行する前記ステップとは、

mビットの第2の値を生成するために、前記n-mビットの第1の中間値(R)を第2のランダム関数(h)に与えるステップと、

mビットを有する前記第2の中間値(T)を生成するために、前記mビットの第1の鍵値(KEY1)と前記mビットの第2の値とにおいて排他的論理和(220)を実行するステップとを含むことを特徴とする請求項3に記載の方法。

【請求項5】 前記第2の中間値(T)の少なくとも一部を与える前記ステップと、前記第2の鍵値(KEY2)の少なくとも第1の部分を生成する前記ステップとは、

n-mビットの第3の値を生成するために、前記mビットの第2の中間値(T)を第3のランダム関数(g)に与えるステップと、

前記第2の鍵値(KEY2)のn-mビットの部分

(V)を生成するために、前記n-mビットの第3の値と、前記n-mビットの第1の中間値(R)とにおいて排他的論理和(240)を実行するステップとを含むことを特徴とする請求項4に記載の方法。

【請求項6】 nビットを有する前記第2の鍵値(KEY2)のmビットの第2の部分として、前記mビットの第2の中間値(T)を与えるステップを含むことを特徴とする請求項5に記載の方法。

10 【請求項7】 前記第3の値を生成するために、前記第2の鍵値(KEY2)の前記第2の部分(T)を、前記第3のランダム関数(g)に与えるステップと、前記第2の鍵値(KEY2)の前記第1の部分(V)と、前記第3の値との排他的論理和(260)をとることにより、前記第1の中間値(R)を生成するステップとを含むことを特徴とする請求項2に記載の方法。

【請求項8】 前記第1の中間値(R)から前記第2の値を生成するために、前記第2のランダム関数(h)を用いるステップと、

20 前記第2の値と、前記第2の鍵値(KEY2)の前記第2の部分(T)との排他的論理和(280)をとることにより、前記第1の鍵値の少なくとも一部を生成するステップとをさらに含むことを特徴とする請求項7に記載の方法。

【請求項9】 第1の通信システムのための第1の鍵値(KEY1)を第2の通信システムのための第2の鍵値(KEY2)に変換するための鍵変換システムであって、

30 第1のランダム関数(f)を用いて、前記第1の鍵値(KEY1)の少なくとも一部から第1の中間値(R)を生成し、前記第1の中間値(R)の少なくとも一部を第2のランダム関数(h)に与えて第2の値を生成するように構成され、前記第1の鍵値(KEY1)の少なくとも一部と前記第2の値の少なくとも一部とについての排他的論理和(220)を実行し、第2の中間値(T)を生成するように構成され、前記第2の中間値(T)の少なくとも一部を第3のランダム関数(g)に与えて、第3の値を生成するように構成され、さらに前記第3の値の少なくとも一部と、前記第1の中間値(R)の少なくとも一部との排他的論理和(240)をとることにより前記第2の鍵値(KEY2)の少なくとも第1の部分を生成するように構成される処理回路を含むことを特徴とする鍵変換システム。

40 【請求項10】 前記処理回路はさらに、前記第2の鍵値(KEY2)の少なくとも第2の部分として、前記第2の中間値(T)の少なくとも一部を生成するように構成されることを特徴とする請求項9に記載のシステム。

【発明の詳細な説明】

【0001】

50 【発明の属する技術分野】 本発明は通信に関し、より具

体的には、無線ユニットが第1の通信システムと第2の通信システムとの間でローミングする際の、第1および第2の通信システムのための鍵の変換に関する。

【0002】

【従来の技術】図1は、地理的なエリア14および16内にそれぞれ位置する無線ユニット（たとえば、無線ユニット12a～c）に無線通信サービスを提供する第1および第2の無線通信システムの概略図である。移動体交換局（たとえば、MSC20および24）は、特に、無線ユニット間の呼、無線ユニットと有線ユニット（たとえば、有線ユニット25）との間の呼、および／または無線ユニットと、インターネットのようなパケットデータ網（PDN）との間の接続を確立し、かつ維持するための役割を担う。そのような場合に、MSCは、その地理的なエリア内にいる無線ユニットを、公衆交換電話網（PSTN）28および／またはパケットデータ網（PDN）29と相互に接続する。MSCによってサービスを提供される地理的なエリアは、「セル」と呼ばれる空間的に個別のエリアに分割される。図1に示されるように、各セルは、蜂の巣状のパターン内の1つの六角形によって概略的に表される。しかしながら、実際には、各セルは、セルを包囲する土地の地形に応じて不規則な形状を有する。

【0003】典型的には、各セルは、無線機とアンテナとを備える基地局（たとえば、基地局22a～eおよび26a～e）を含み、基地局はそれを用いて、そのセル内の無線ユニットと通信を行う。また基地局は、基地局が地理的なエリア内のMSCと通信するために用いる伝送装置も備える。たとえば、MSC20は、地理的なエリア14内の基地局22a～eに接続され、MSC24は、地理的なエリア16内の基地局26a～eに接続される。地理的なエリア内では、無線ユニットがセル間を移動する、すなわち呼をハンドオフするのに応じて、MSCは基地局間でリアルタイムに呼を切り替える。実施形態によっては、基地局コントローラ（BSC）として、いくつかの基地局に接続されるか、あるいは各基地局に配置され、その基地局のための無線リソースを管理し、かつMSCに情報を中継する個別の基地局コントローラ（BSC）（図示せず）を用いることができる。

【0004】MSC20および24は、「Cellular Radiotelecommunications Intersystem Operations」（1997年12月、「IS-41」というタイトルのTIA/EIA-41-Dとして規定される標準規格に準拠するシグナリングネットワークのような、シグナリングネットワーク32を用いており、そのネットワークによって、各地理的なエリア14および16内でローミングしている無線ユニットについての情報を交換できるようになる。たとえば、無線ユニット12aが、最初に割り当てられたMSC20（たとえば、ホームMSC）の地理的なエリア14から離れる際に、無線ユニット12a

はローミング状態になる。ローミング中の無線ユニットが呼を確実に受信できるようにするために、ローミング無線ユニット12aは、自分の存在をビジターMSC24に知らせることにより、現時点で自分が在籍しているMSC24（ビジターMSC）で登録を行う。一旦、ビジターMSC24によってローミング中の無線ユニット12aが識別されたなら、ビジターMSC24は、シグナリングネットワーク32を介して、ホームMSC20に登録要求を送信し、ホームMSC20は、そのビジターマスク24の識別情報を用いて、ホームロケーションレジスタ（HLR）と呼ばれるデータベース34を更新し、それにより、ローミング中の無線ユニット12aの位置がホームMSC20に提供される。

【0005】ローミング中の無線ユニットが認証された後、ホームMSC20はビジターMSC24に、コールウェイティング、発信者番号通知、着信転送、三者通話、国際通話のような、ローミング中の無線ユニットが利用できる機能を指示する顧客プロファイルを提供する。顧客プロファイルを受信すると、ビジターMSC24は、ビジターロケーションレジスタ（VLR）と呼ばれるデータベース36を更新し、ホームMSC20と同じ機能を提供する。HLR、VLRおよび／または認証局（AC）は、MSCと同じ場所に配置されることができるか、あるいはリモートでアクセスされることができる。

【0006】無線ユニットが、異なる無線通信標準規格を用いる無線通信システム間でローミングしている場合には、異なる無線通信システムにおいて、無線ユニットに同じ機能およびサービスを提供することは、実現可能ではあるが、複雑になる。現在、米国、欧州および日本では、異なる無線通信標準規格が用いられている。現在、米国は、異なる標準規格を用いる2つの無線通信システムを主に用いている。第1のシステムは、時分割多元接続（TDMA）システムであり、IS-136として知られる標準規格によって規定されている。第2のシステムは、符号分割多元接続（CDMA）システムであり、IS-95として知られる標準規格によって規定される。いずれの通信システムとも、システム間メッセージ伝送のために、認証手順を規定するIS-41として知られる標準規格を用いる。

【0007】TDMAシステムでは、ユーザは周波数帯を共有し、各ユーザの音声は、ユーザを区別するように制御されたタイムスロットを用いて、高速パケットとして格納され、圧縮され、かつ伝送される。それゆえ「時分割」と呼ばれる。受信機側では、そのパケットの圧縮が解除される。IS-136プロトコルでは、3人のユーザが所与の搬送波周波数を共有する。対照的に、CDMAシステムは、固有の符号を用いて、広い領域のスペクトルにわたって信号を「拡散」し（それゆえ、別名、スペクトル拡散と呼ばれる）、受信機は同じ符号を用い

て、雑音から信号を再生する。極端に低い電力の信号の場合でも、非常に耐雑音性の、確実なチャネルを確立することができる。さらに、異なる符号を用いることにより、多数の異なるチャネルが、互いに干渉することなく、同時に同じ搬送波信号を共有することができる。CDMAおよびTDMAはいずれも、ユーザ情報のプライバシーあるいは秘密性のために異なる要件を有する第2世代(2G)および第3世代(3G)フェーズの場合に規定されている。

【0008】欧洲は、欧洲電気通信標準化機構(ETSI)によって規定されるような移動体のためのグローバルシステム(GSM)ネットワークを用いる。GSMはTDMA標準規格であり、8人のユーザが搬送波周波数を共有する。音声は20msの窓で取り込まれ、サンプリングされ、処理され、かつ圧縮される。GSMは900MHz帯の搬送波上で伝送される。別のシステムは1.8GHz帯で動作し(DCS1800)、付加的な容量を提供しており、それは、セルラーシステムではなく、パーソナル通信システム(PCS)の多くで頻繁に用いられている。同じように、米国でもDCS-1900、すなわち1.9GHzの異なる搬送波上で動作する別のGSMシステムが実施されている。パーソナルデジタルセルラー(PDC)は日本の標準規格であり、以前にはJDC(日本デジタルセルラー)として知られていた。PDCは、IS-54プロトコルとして知られている米国標準規格と同様のTDMA標準規格である。

【0009】GSMネットワークは、クレジットカードサイズの着脱式のユーザ識別モジュール(UIM)を用いており、そのモジュールは加入者が所有し、加入者はUIMをGSMハンドセットに挿入して、そのハンドセットを自分の電話として用いる。加入者の固有の電話番号がダイヤルされるときに呼出音が鳴動し、通話料はその加入者の口座に課金されるであろう。全てのオプションおよびサービスに接続することができ、ボイスメール等にも接続することができる。異なるUIMを所持する加入者が1台の「物理的な」ハンドセットを共有し、それを、UIM毎に1台の、いくつかの「仮想的な」ハンドセットに変えることができる。また、米国のシステムと同様に、GSMネットワークによれば、他の無線通信システムあるいはネットワークからの加入者を認識する(および受け入れる)ことに合意している種々のネットワーク事業者によって、無線ユニット(あるいはUIM)が移動する際に「ローミング」が可能になる。そこで、イギリスの加入者が、フランスあるいはドイツ国内をドライブしながら、GSM無線ユニットを用いて(同じイギリスの電話番号で)発着呼することができ、それは、米国の無線通信システムの任意のシステムにおいて、米国のビジネスマンがボストン、マイアミあるいはシアトルで無線ユニットを用いることができるのと同じように簡単である。そのGSMシステムは、第2世代

(2G)システムとして規定される。

【0010】GSMセキュリティ方式の第3世代における改善は、ユニバーサル移動体電気通信サービス(UMTS)の一式の標準規格において、特に3GPP TS-33.102「セキュリティアーキテクチャ」仕様書として特定される標準規格のセキュリティの場合に規定されている。わずかな変形方式を有するこのセキュリティ方式は、UMTS、TDMAおよびCDMAを含む全ての3G通信システムのための世界的に共通のセキュリティ方式の基本方式として用いられるであろう。

【0011】2G-GSM認証方式が図2に示される。この認証方式は、ホームロケーションレジスタ(HLR)40と、ビジターロケーションレジスタ(VLR)50と、UIM62を含む無線ユニットあるいは移動端末(MT)60とを含む。移動端末60が電話を掛けるとき、ホームロケーションレジスタ40に要求が送信され、ホームロケーションレジスタ40は、ルート鍵K₁から、「トリプレット」(RAND、SRES、K₁)とも呼ばれる認証ベクトルAVを生成する。トリプレットはランダム数RANDと、符号付きの応答SRESと、セッション鍵K₁とを含む。トリプレットはビジターロケーションレジスタ50に与えられ、ビジターロケーションレジスタ50はそのランダム数RANDを移動端末60に渡す。UIM62はランダム数RANDを受信し、ルート鍵K₁、ランダム数RAND、およびアルゴリズムA3を用いて、符号付きの応答SRESを計算する。また、UIM62は、ルート鍵K₁、ランダム数RAND、およびアルゴリズムA8を用いて、セッション鍵K₁も計算する。UIM62によって計算されたSRESは、ビジターロケーションレジスタ50に返送され、ビジターロケーションレジスタ50は移動端末30を用いる加入者を認証するために、ホームロケーションレジスタ40から受信されたSRESからの値と比較する。

【0012】GSM「チャレンジ/応答」認証システムでは、ビジターロケーションレジスタ50は、UIM32およびホームロケーションレジスタ40によって保持されているルート鍵K₁を受信することはない。またVLR50は、HLR40およびUIM62によって用いられる認証アルゴリズムを知る必要もない。また、GSM認証方式では、トリプレットは、ホームロケーションレジスタ40によって呼び出される全ての電話の場合に送信されなければならない。RANDは128ビットであり、SRESは32ビットであり、K₁は64ビットであり、各要求の場合に224ビットのデータになり、著しいデータ負荷になる。この説明の主な焦点は、ユーザ情報の秘密性のために用いられる、64ビット長K₁セッション暗号化鍵である。通話中に、移動端末が別のサービス提供システムにローミングするとき、セッション鍵K₁は、古いVLRから新しいターゲットサービス

提供システムに転送される。

【0013】図3は、2G GSM方式に対して改善されたUMTSセキュリティ方式を示す。GSM方式と同様に、移動端末90が電話を掛けるとき、ホームロケーションレジスタ70に要求が送信され、ホームロケーションレジスタ70は認証ベクトルAVを、トリプレットの3つの要素の代わりに5つの要素、それゆえ「クインタプレット」と呼ばれる要素を含むビジターロケーションレジスタ(VLR)80に送信する。このベクトルは、128ビットRANDと、64ビットSRESと、ホームネットワークの認証サインおよび2つのセッションセキュリティ鍵を有するAUTN値と、128ビット暗号化鍵CKと、128ビット完全性確認(integrity)鍵IKとを含む。これらのうちの後者の2つの鍵、CKおよびIKがこの説明の焦点である。

【0014】そのベクトルはビジターロケーションレジスタ80に与えられ、ビジターロケーションレジスタ80は、ランダム数RANDおよびAUTNを移動端末に渡す。UIM92はランダム数RANDを受信し、ルート鍵K₁と、ランダム数RANDと、所定のアルゴリズム関数とを用いて、AUTNの妥当性を検査し、符号付の応答SRESを計算する。またUIM92は、ルート鍵K₁と、ランダム数RANDと、所定のアルゴリズム関数とを用いて、セッション鍵CKおよびIKも計算する。UIM92によって計算されたSRESは、ビジターロケーションレジスタ80に返送され、ビジターロケーションレジスタ80は、移動端末90を用いる加入者を認証するために、ホームロケーションレジスタ70から受信されたSRESからの値と比較する。この説明の焦点は、128ビット長セッション暗号化鍵CKと、128ビット長セッション完全性確認鍵IKとにあり、それらは、ユーザ情報の秘密性と、セッション完全性の保護とのために用いられる。一旦、加入者が認証に成功したなら、VLR80は、この認証ベクトルにおいて受信されたCKおよびIKを有効にする。通話中に、移動端末が別のサービス提供システム内にローミングする場合には、CKおよびIKは新しいターゲットサービス提供システムに送信される。

【0015】米国TDMAおよびCDMAシステムにおいて用いられる、2G IS-41認証方式が図4に示される。この認証方式は、ホームロケーションレジスタ(HLR)100と、ビジターロケーションレジスタ(VLR)110と、UIM122を含むことができる移送端末(MT)120とを含む。A_鍵として知られるルート鍵は、HLR100およびUIM122内にのみ格納される。共有秘密データSSDとして知られる補助鍵が存在し、ローミング中にVLR110に送信される。SSDは、暗号作成アルゴリズムを用いてA_鍵から生成される。SSDを生成するための手順は他でも記載されており、当業者には知られている。MT120が

訪問先のネットワークにローミングするとき、VLR110はHLR100に認証要求を送信し、HLR100は、その加入者のSSDを送信することにより応答する。一旦、VLR110がそのSSDを所持したなら、VLR110は、HLR100とは無関係に、あるいは当業者に知られているようにHLR100の支援を受けて、MT120を認証することができる。VLR110はMT120を介して、ランダム数RANDをUIM122に送信し、UIM122はRANDと、UIM122に格納されたSSDの値とを用いて、認証応答(AUTHR)を計算する。AUTHRはVLR110に返送され、VLR110は、同じようにして個別に計算されたAUTHRの値に対して、そのAUTHRを検査する。2つのAUTHR値が一致する場合には、MT120が公然と有効になる。このプロセスは、無線ユニットがそのシステムにアクセスしようとするとき、たとえば、発呼しようとするとき、あるいは着呼に対して応答するときに繰り返される。

【0016】これらの場合に、セッションセキュリティ鍵も生成される。セッションセキュリティ鍵を生成するために、認証計算が行われた後に、計算アルゴリズムの内部状態が保持される。その後、現在のSSDの値を用いて、UIM122およびVLR110によって、いくつかのセッションセキュリティ鍵が計算される。具体的には、520ビットの音声秘話マスク(VPM)が計算され、それが、通話中にTDMA音声データを盗聴されないように用いられる。このVPMは、UIMおよびVLRによって呼の開始時に導出され、移動端末が通話中に別のサービス提供システムにローミングする場合には、VPMは、VLRによって新しいサービス提供システムに送信される。呼が終了するとき、VPMは、UIMおよびサービス提供VLRの両方によって消去される。同様に、64ビットシグナリングメッセージ暗号鍵(SMEKEY)が計算され、通話中にTDMAシグナリング情報を暗号化するために用いられる。このSMEKEYは、UIMおよびVLRによって呼の開始時に導出され、移動端末が通話中に別のサービス提供システムにローミングする場合には、SMEKEYは、VLRによって新しいサービス提供システムに送信される。呼が終了するとき、SMEKEYは、UIMおよびサービス提供VLRの両方によって消去される。

【0017】2G CDMA方式は類似の方法による鍵分配を用いるが、520ビットVPMの代わりに、プライベートロングコードマスク(PLCM)への発生源として、VPMの42最下位ビット(LSB)を用いている。このPLCMは、拡散前の情報のための付加的なスクランブルマスクとして用いられる。42ビットPLCMは通話中に不变であり、移動端末が別のサービス提供システムにローミングする場合には、VLRによって新しいサービス提供システムに送信される。SMEKEY

は、TDMA系の方式と同じように用いられる。

【0018】IS-41-3Gセキュリティ方式はUMTSセキュリティ方式を用いており、それは、UIMによって同じ鍵が計算される間に、128ビット暗号化鍵CKおよび128ビット完全性確認鍵IKが、訪問されたシステムのVLRに給送されることに基づく。

【0019】無線ユニットが通信システム間でローミングする際の鍵変換は、セキュリティが低い2G方式およびアルゴリズムが混在し、侵入者によって鍵が部分的に再生される場合であっても、3Gセッション鍵が依然として同じセキュリティのレベルを保持することになるように実行されるべきである。そのような変換によって、加入者は、通信データのセキュリティおよび通信セッションの完全性を保持しながら、「広域にわたってローミング」できるようになるであろう。

【0020】

【発明が解決しようとする課題】本発明の目的は、第1の通信システムの第1の鍵値から第2の通信システムの第2の鍵値に、決定論的に、かつ可逆的に変換するための鍵変換システムを提供することである。

【0021】

【課題を解決するための手段】たとえば、その鍵変換システムは、第1のランダム関数を用いて、第1の鍵値の少なくとも一部から第1の中間値を生成する。第1の中間値の少なくとも一部は、第2の値を生成するために第2のランダム関数に与えられる。第1の鍵値の少なくとも一部と、第2の値の少なくとも一部とにおいて排他的論理和(XOR)が実行され、第2の中間値が生成される。第2の中間値の少なくとも一部は、第3の値を生成するために第3のランダム関数に与えられる。第3の値の少なくとも一部と、第1の中間値の少なくとも一部とにおいて排他的論理和を実行することにより、鍵変換システムは第2の鍵値の少なくとも第1の部分を生成し、第2の鍵値の少なくとも第2の部分は第2の中間値として生成される。その鍵変換システムは、第1の鍵値を与えるとき、無線ユニットおよび無線通信システムが、情報を交換することを必要とすることなく、同じ第2の鍵値を決定することになるという点で決定論的である。

【0022】その鍵変換システムは、無線ユニットが第1の通信システムにハンドオフして戻る場合には、第2の通信システムの第2の鍵値が、第1の通信システムの第1の鍵値に変換して戻されるという点で可逆的、あるいは双方向的である。たとえば、鍵変換システムは、第2の鍵値の少なくとも第2の部分を第3のランダム関数に与え、第3の値を生成する。第2の鍵値の少なくとも第1の部分と、第3の値とにおいて、排他的論理和を実行することにより、第1の中間値が生成される。第2のランダム関数を用いて、鍵変換システムは、第1の中間値から第2の値を生成し、第2の値と、第2の鍵値の第2の部分とにおいて排他的論理和を実行することによ

り、第1の鍵値の少なくとも一部を生成する。鍵変換システムは、第2の鍵値のほとんど全てがわかっている場合であっても、第1の鍵値を容易には再生することができないので、改善されたセキュリティを提供する。同様に、第1の鍵値のほとんど全てがわかっている場合であっても、第2の鍵値は容易に再生されない。

【0023】本発明の他の態様および利点は、以下に記載される詳細な説明を読み、図面を参照すれば明らかになるであろう。

10 【0024】

【発明の実施の形態】本発明の原理にしたがった鍵変換システムの例示的な実施形態が以下に記載されており、それは、第1の通信システムと第2の通信システムとの間でローミングする無線ユニットのための改善された鍵変換を提供する。鍵変換システムは、第1の通信システムのmビットの鍵値を、第2の通信システムのnビットの鍵値に決定論的、かつ可逆的に変換する。ある実施形態では、その鍵変換システムは、3つのランダム関数f、gおよびhを用いる。ただし、ランダム関数fおよびgは、mビット入力データ列を、ランダム数に類似しているn-mビットデータ列にマッピングし、ランダム関数hは、n-mビットデータ列を、ランダム数に類似しているmビットデータ列にマッピングする。ランダム関数は、入力を与えるときに、出力が予測不可能であり、ランダムに見えるように、入力を出力にマッピングする。以下に記載される実施形態では、ランダム関数はランダムオラクルであり、入力が与えられる度に、同じ出力にマッピングする。また、以下に記載される実施形態において、ランダム関数は既知である。たとえば、ランダム関数は、システム間ハンドオフに関わる無線通信システムと、無線ユニットとによって知られている。

【0025】その鍵変換システムは、mビット鍵値を与えるとき、無線ユニットおよび無線通信システムが、情報の交換を必要とすることなく、同じnビット鍵値を決定することになる点で決定論的である。その鍵変換システムは、無線ユニットがハンドオフして第1の通信システムに戻る場合には、第2の通信システムのnビット鍵が変換され、第1の通信システムのmビット鍵に戻るという点で、可逆的あるいは双方向的である。鍵変換システムは、nビットの鍵値のほとんど全てがわかっている場合であっても、mビットの鍵値を容易には再生することができないので、改善されたセキュリティを提供する。同様に、mビットの鍵値のほとんど全てがわかっている場合であっても、nビットの鍵値は容易には再生されない。

【0026】その実施形態に応じて、無線ユニットが、古い通信システムと新しい通信システムとの間のように、2つの無線通信システム間でローミングする際に、安全で、決定論的で、しかも双方向的な鍵変換システムを提供することができる。たとえば、同じ参照番号が同

様の構成要素を指示する場合、無線ユニットが2G-TDMAシステムから3Gシステムにローミングする際に、図5のIS-41-3Gセキュリティ方式は、VLR80および無線ユニット120（あるいは122）において、520ビットVPMをVLR110から受信された64ビットSMEKEYと組み合わせて、128ビットCKおよび／または128ビットIKに変換する。逆に、図6に示されるように、無線ユニットが3Gシステムから2G TDMAシステムにローミングする際に、IS-41-3Gセキュリティ方式は、VLR80および無線ユニット90（あるいは92）において、128ビットCKおよび／または128ビットIKを、64ビットSMEKEYと組み合わせた520ビットVPMに変換する。VLR80は、VPMおよびSMEKEYをVLR110に提供する。

【0027】図7に示されるように、無線ユニットが2G-CDMAシステムから3Gシステムにローミングする際に、IS-41-3Gセキュリティ方式は、VLR80および無線ユニット120（あるいは122）において、42ビットPLCMをVLR110から受信された64ビットSMEKEYと組み合わせて、128ビットCKおよび／または128ビットIKに変換する。逆に、図8に示されるように、無線ユニットが3Gシステムから2G-CDMAシステムにローミングする際に、IS-41-3Gセキュリティ方式は、VLR80および無線ユニット90（あるいは92）において、128ビットCKおよび／または128ビットIKを、64ビットSMEKEYと組み合わせた42ビットPLCMに変換する。VLR80は、PLCMおよびSMEKEYをVLR110に提供する。

【0028】図9に示されるように、無線ユニットが2G-GSMシステムから3G-UMTSシステムにローミングする際に、UMTS-3Gセキュリティ方式は、VLR80および無線ユニット60（あるいは62）において、VLR50から受信された64ビットK。を、128ビットCKおよび／または128ビットIKに変換する。逆に、図10に示されるように、無線ユニットが3G-UMTSシステムから2G-GSMシステムにローミングする際に、UMTS-3Gセキュリティ方式は、VLR80および無線ユニット90（あるいは92）において、128ビットCKおよび／または128ビットIKを、64ビットK。に変換する。VLR80は、K。をVLR50に提供する。

【0029】したがって、ある実施形態では、新しい3G通信システムのような、第1の通信システムにおいて、改善された加入者認証（ESA）および改善された加入者プライバシー（ESP）に対応する無線ユニットは、多数のプライバシーモードを実装し、古い2G-TDMA通信システムのような、第2の通信システムにおいて、無線ユニットが古いアルゴリズムを用いるプライ

バシーを提供できるようにする。そのような無線ユニットは、ESPに対応しない古い第2の通信システムの場合に、MSCへのシステム間ハンドオフの後に、他の形式のプライバシーを提供することができる。古い第2の通信システムへのハンドオフが必要とされるとき、鍵変換システムは、新しい第1の通信システムのための鍵値を、古い第2の通信システムが対応する古いプライバシーアルゴリズムのために必要とされる秘密鍵に変換することができる。第2の通信システムのための鍵は、第1の通信システムのMSCから、第2の通信システムのターゲットMSCに送信されることができる。鍵変換システムは決定論的であるため、無線ユニットも、本発明の鍵変換システムを用いる第1の通信システムと同じ変換を実行することにより、第2の通信システムのための鍵を有することになるであろう。

【0030】その鍵変換システムは、第1のシステムからの鍵を第2のシステムからの鍵にマッピングし、さらに再び元に戻す。たとえば、3G通信システムと2G-TDMAシステムとの間でシステム間ハンドオフを実行する際に、その鍵変換システムは、暗号鍵CKを、VPMASK/SMEKEY(VS)対にマッピングすることができる。この実施形態では、鍵変換機能は以下の特性を有する。1) 128ビットCKは584ビットVSにマッピングされる。2) その機能は可逆的であり、583ビットVSが128ビットCKに逆にマッピングされる。3) その機能は、584ビット鍵の一部がわからても、侵入者がCKを再生できないようになるか、128ビット鍵CKの一部がわからても、侵入者が584ビットVSを再生できないようになる意味で安全である。30 ある例では、たとえば、ターゲットの第2の通信システムより大きな鍵値を有する第1の通信システムにおいて発呼する際に、その変換システムは、第1の通信システムの鍵値を、第2の通信システムの鍵値にマッピングする。しかしながら、無線ユニットが第1の通信システムに戻る場合には、その鍵変換システムは、第2の鍵値を、第1の通信システムのための後続の鍵値にマッピングするが、その鍵値は最初の鍵値と必ずしも同じではない。第2の通信システムから第1の通信システムに戻る、その後のハンドオフは、後続の鍵値と同じである鍵値を生成する。

【0031】たとえば、2G-TDMAシステムで発呼する場合、3Gシステムへのシステム間ハンドオフを実行する際に、鍵変換システムは、VPMASK/SMEKEY(VS)対を暗号鍵CKにマッピングすることができる。この実施形態では、鍵変換機能は、584ビットVSを128ビットCKにマッピングする。無線ユニットが2G-TDMAシステムにハンドオフして戻る場合には、鍵変換システムは、128ビットCKを584ビットVSにマッピングして戻すが、新しい584ビットVSは、最初の584ビットVSと同じではない場合

がある。3Gシステムから2G TDMAシステムへの後続のハンドオフは新しい584ビットVSを保持するであろう。これは、無線ユニットのセキュリティあるいは動作を達成しない場合であっても、この実施形態では、128ビットCKは常に同じ値に保持される。

【0032】この実施形態では、鍵変換システムは、新しいシステム内のMSCおよび無線ユニットにおいて利用可能な変換機能を含み、変換機能は、第1の通信システムのための、ESP鍵のような鍵値を、古いプライバシー・アルゴリズムのために用いられる鍵のような、第2の通信システムの鍵値に変換するであろう。この例では、その変換機能は、新しい第1の通信システムにおける128ビットCKを、古い第2の通信システムのためのVPMASK/SMEKEY(VS)鍵に変換することになる。VPMASKは各方向の場合に260ビットマスクからなり、SMEKEYは、古い通信システムによって用いられる全584ビットの場合に64ビット長である。古い通信システムから新しい通信システムへのシステム間ハンドオフの場合には、変換機能が可逆的であることが有用な場合がある。古い通信システムは新しい通信システムについての情報を持たず、584ビット全てを新しい通信システムに転送するであろう。584ビット鍵の受信時に、新しい通信システムは、128ビットCKを再生する必要があることを理解し、それゆえ、584ビット鍵からCKを計算するであろう。

【0033】無線ユニットおよびMSCにおいて作成されるVS鍵は同じになるべきである。これは、VS鍵の計算が、CKと、MSCおよび無線ユニットの両方において知られている任意の他の量とにのみ基づかなければならぬことを意味する。そうでなければ、任意の新しい量（たとえば、ランダム数）が、変換前に、無線ユニットとMSCとの間で交換されなければならないであろう。その鍵変換システムは、無線ユニットと新しいMSCとの間で情報を交換することを必要とせず、CKをVS鍵に、かつVS鍵をCK鍵に決定論的にマッピングする。

【0034】さらに、古い通信システム内の弱点によって、新しい通信システムが影響を受けることはないようすべきである。これは、一方向に暗号化技術を用いて変換機能を実施することにより達成することができ、その結果、この例ではVS鍵のような古い通信システムの鍵全体が漏洩される場合であっても、侵入者は、この例ではCK鍵のような新しい通信システムの鍵を再生することができない。しかしながら、これはそのシステムを不可逆的にすることになり、上記のように、鍵変換システムは可逆的でなければならない。それにもかかわらず、鍵変換システムは可逆的にすることができ、依然として、不可逆的な機能のセキュリティのほとんど全てを提供することができる。この例における鍵変換システムのセキュリティは、小さな部分を除いて、VS鍵のほと

んど全てが漏洩される場合でも、侵入者がCK鍵のあらゆる部分を再生するのを防ぐ。侵入者はその小さな部分を推測することはできるが、それ以上先に進むことはできない。この態様は、VPMASKの一部が他の部分より容易に再生される場合があり、VPMASK全体がSMEKEYより容易に再生される場合があるので重要である。さらに、古いシステムのある部分を再生するのが難しい場合には、侵入者はCKについて何もわからることはないであろう。同様のセキュリティは、CKが部分的にわかつても、侵入者がVSについて何も知ることができないように、CKにも適用することができる。

【0035】ある実施形態では、その変換機能は2つのモード、すなわち順方向変換および逆方向変換を有する。3G通信システムから2G TDMA通信システムへのローミングの例では、順方向変換機能は、128ビットのランダムに作成されたCK鍵を受け取り、それを584ビットVS鍵に拡張する。逆方向変換機能は、584ビットVS鍵を受け取り、それを128ビットCK鍵にマッピングする。この実施形態では、順方向変換機能は、所与の入力をランダムな出力にマッピングする3つのランダム関数f、gおよびhからなる。この実施形態では、これらは秘密の機能ではなく、侵入者を含む誰でもが知ることができる公開されたランダム関数である。これらの公開ランダム関数は、本明細書ではランダムオラクルと呼ばれる。これらのランダムオラクルは、以下に記載されるように、ハッシュ関数およびブロック暗号を用いて実施されることができる。この例では、3つのランダム関数はf、gおよびhであり、fおよびgは128ビット入力を456ビットランダム値にマッピングし、hは456ビット入力を128ビットランダム値にマッピングする。

【0036】図11は、第1の通信システムのmビット鍵値KEY1を第2の通信システムのnビット鍵値KEY2に変換するための鍵変換システムの順方向変換の一実施形態の流れ図を示す。mビットKEY1は、ランダム関数f（ブロック200）に与えられ、ランダム関数fはmビットデータ列を、n-mビットランダム数あるいは第1の中間値Rにマッピングする。3G通信システムから2G TDMA通信システムにローミングする例では、変換システムは、128ビット鍵CKを584ビット鍵（VPMASK、SMEKEY）に変換する。128ビット鍵CKは、ランダム関数f（ブロック200）に与えられ、ランダム関数fは128ビットCKを、456ビットランダム数あるいは第1の中間値Rにマッピングする。中間値Rはランダム関数h（ブロック210）に与えられ、ランダム関数hは、n-mビットデータ列をmビットランダム数にマッピングする。関数h（210）のmビット出力は、mビットKEY1と排他的論理和（XOR220）をとられ、mビットの第2の中間値Tが生成される。3G通信システムから2G T

DMA通信システムにローミングする例では、456ビット中間値Rは関数h(210)に与えられる。関数h(210)は456ビット値Rを128ビットランダム数にマッピングし、そのランダム数は128ビットCKとの排他的論理和をとられ、128ビットの第2の中間値Tが生成される。

【0037】図11の実施形態では、mビット中間値Tは、ランダム関数g(ブロック230)に与えられる。ランダム関数g(ブロック230)は、mビットデータ列をn-mビットランダム数にマッピングし、そのランダム数はn-mビット中間値Rと排他的論理和(XOR240)をとられ、1つの鍵、複数の鍵あるいは鍵の一部として用いることができるn-mビット鍵値Vが生成される。この実施形態では、値Vは、1つの鍵、複数の鍵あるいは鍵の一部として用いることができる値KEY2の一部である。この実施形態では、nビット鍵KEY2は、mビットの第2の中間値Tとともに、n-mビット値Vを含む。3G通信システムから2G TDMA通信システムにローミングする例では、ランダム関数g(230)は128ビット中間値Tを456ビットランダム数にマッピングし、そのランダム数は456ビット中間値Tとの排他的論理和(XOR240)をとられ、456ビット鍵値Vが生成される。456ビット値Vおよび128ビット中間値Tは、この例では、2G TDMAシステムのためのVPMASKおよびSMEKEYに分割することができる584ビット鍵値KEY2を形成する。

【0038】3GシステムのCKから2G TDMAシステムのVPMASKおよびSMEKEYへの順方向変換は、以下のステップにより書き表すことができる。

1. $R = f(CK)$ /* fを適用することにより128ビットCKから456ビット値を作成*/
2. $T = h(R) \text{ XOR } CK$ /* hを用いて128ビット値を作成*/
3. $V = g(T) \text{ XOR } R$ /* gを用いて456ビット値を作成*/
4. 出力T, V /* 584ビット値を出力*/

【0039】図12は、第2の通信システムのnビット鍵値KEY2を、第1の通信システムのmビット鍵値KEY1に変換して戻すための鍵変換システムの逆方向変換の一実施形態の流れ図である。この実施形態では、nビット鍵値KEY2は、n-mビットの第1の部分あるいは値Vと、mビットの第2の部分あるいは値Tとに分割される。mビット値Tは、ランダム関数g(ブロック250)に与えられ、ランダム関数gは、mビットデータ列をn-mビットランダム数にマッピングする。n-mビットランダム数は、n-mビット鍵値Vと排他的論理和(XOR260)をとられ、n-mビットの第1の中間値Rが生成される。無線ユニットが3Gシステムから2G TDMAシステムにローミングして戻る例で

は、変換システムは、584ビット鍵(VPMASK、SMEKEY)を128ビット鍵CKに変換する。128ビット鍵値部分Tは、ランダム関数g(ブロック250)に与えられ、ランダム関数gは128ビットTを456ビットランダム数にマッピングする。456ビットランダム数は、456ビット鍵値Vと排他的論理和(XOR260)をとられ、456ビットの第1の中間値Rが生成される。

【0040】図12の実施形態では、n-mビットの第1の中間値Rはランダム関数h(ブロック270)に与えられる。ランダム関数h(ブロック270)は、n-mビットデータ列をmビットランダム数にマッピングし、mビットランダム数は、mビット鍵値Tと排他的論理和(XOR280)をとられ、1つの鍵、複数の鍵あるいは鍵の一部として用いることができるmビット鍵値KEY1が生成される。無線ユニットが3Gシステムから2G TDMAシステムにローミングして戻る例では、ランダム関数h(ブロック270)は、456ビット中間値Rを128ビットランダム数にマッピングし、128ビットランダム数は、128ビット鍵値Tと排他的論理和(XOR280)をとられ、128ビット鍵CKが生成される。

【0041】2G TDMAシステムのVPMASKおよびSMEKEYから3GシステムのCKへの逆方向変換は、以下のステップにしたがって書き表すことができる。

1. T, Vを584ビット入力に設定 /* Tは128ビット部分、Vは456ビット部分*/
2. $R = g(T) \text{ XOR } V$ /* T, Vを用いて456ビット値Rを作成*/
3. $CK = h(R) \text{ XOR } T$

【0042】ランダム関数f、gおよびhは、ハッシュ関数および/またはブロック暗号を用いて実装することができます。ランダムオラクルと呼ぶことができる、ランダム関数f、gおよびhを実装するために、SHA-1、MD5、RIPE-MDとして知られる関数のような暗号作成ハッシュ関数を用いて、ランダム関数f、gおよびhを具現することができる。ハッシュ関数は典型的には、ある長さの入力を別の長さの出力にマッピングする関数として特徴付けることができ、ある出力を与えるときに、その所与の出力にマッピングすることになる入力を判定するのは不可能である。さらに、同じ出力にマッピングすることになる2つの入を見つけることはできない。SHA-1ハッシュ関数を用いる場合、SHA-1ハッシュ関数への各呼出しは160ビット初期ベクトル(IV)を有し、160ビット出力にマッピングされる512ビット入あるいはペイロードを要する。IVはSHA-1ハッシュ関数のための標準規格に定義されるIVに設定される。ペイロードは、種々の入力引数、SHA(Type, Count, Input, Pa

d) を含むであろう。ただし Type は種々の関数 f、g、h を定義する 1 バイト値である。関数 f および g は SHA を何度も呼び出すことになり、Count は多数の呼出しを区別する 1 バイト値である。Input は関数 f、g あるいは h への入力引数である。Pad は 512 ビット SHA ベイロード内の残りのビット部分を埋めるための 0 値である。以下に記載されるのは、SHA と呼ばれるハッシュ関数ルーチンを用いて、ランダム関数 f、g および h を実装するための手順の一例である。

SHA (Type, Count, Input, Pad)

f (CK) : SHA (1, 1, CK, pad)

SHA (1, 2, CK, pad)

SHA (1, 3, CK, pad) mod 2¹³⁶

h (R) : SHA (2, 1, R, pad) mod 2¹²⁸

g (T) : SHA (3, 1, T, pad)

SHA (3, 2, T, pad)

SHA (3, 3, T, pad) mod 2¹³⁶

AES のようなブロック暗号を用いて、関数 f、g および h を作成することができる。

f (CK) : E_{CK} (1) ; E_{CK} (2) ; E

{CK} (3) ; E{CK} (4) mod 2⁷²

h (R) : E_{CK} (R1 XOR 5) XOR E_{CK}

(R2 XOR 6) XOR E_{CK} (R3 XOR

7) XOR E_{CK} (R4 XOR 8)

g (T) : E_T (9) ; E_T (10) ; E_T (11) ;

E_T (12) mod 2⁷²

ただし、f (CK)において、CK はブロック暗号内の鍵として用いられ、512 ビットストリームはカウンタモードにおいて 1...4 を暗号化することにより生成される。最後の暗号は 128 ビットから 72 ビットに打ち切られ、必要とされる 456 ビットが得られる。h (R)において、公開鍵 K0 は、456 ビット R の部分を暗号化するために用いられ、結果的に生成された暗号列が互いに排他的論理和をとられる。R1、R2 および R3 は 128 ビット値であり、R4 は R の残りの 72 ビット値であり、128 ビットを完成させるために 0 で埋められる。

【0043】こうして、鍵変換システムは、第 1 の通信システムと第 2 の通信システムとの間の鍵あるいはその一部の双方向的で、決定論的で、安全な変換を提供する。その鍵変換システムは、出力 KEY2 (たとえば、T、V) の大部分が与えられるときでも、侵入者が KEY1 (たとえば、CK) を再生することができないという点で、順方向において安全である。2G TDMA と 3G システムを用いる例では、T の全て、および、たとえば 64 ビットを除く V の大部分が知られる場合であっても、R = g (T) XOR V を計算することによって、R の一部は再生することができるが、R を全て再生できるわけではない。CK = h (R) XOR T を実

行することにより、CK のある部分を再生しようと試みることができる。しかしながら、R の全てがわかるわけではないため、h がランダム関数であるものと仮定すると、h (R) について情報の 1 ビットたりとも再生することができない。それゆえ、CK について情報を再生することはできない。同様に、V の全てと、たとえば T の 64 ビットを除く T の一部がわかる場合であっても、CK についての情報を再生することはできない。T の全てがわかるわけではないため、g (T) XOR V を用いて中間値 R を計算することはできない。したがって、中間値 R を用いなければ、CK についてのあらゆる情報を再生する場合に、先に進むことができない。

【0044】同様に、その鍵変換システムは、出力 KEY1 (たとえば、CK) の大部分が与えられても、侵入者が KEY2 (たとえば、T、V) を再生することができないという点で逆方向において安全である。たとえば、2G TDMA および 3G システムを用いる例では、CK の一部がわかる場合であっても、T、V についての情報を再生することはできない。CK の全てがわかるわけではないため、f (CK) を用いて中間値 R を計算することはできない。したがって、中間値 R を用いなければ、T、V についてのあらゆる情報を再生する場合に、先に進むことができない。

【0045】上記の実施形態に加えて、本発明の原理にしたがった鍵変換システムは、入力パラメータおよび/またはランダム関数あるいは他の操作を省略し、かつ/または追加して、かつ/または記載されたシステムの変形あるいは一部を使用して用いることができる。たとえば、鍵変換システムは、ランダムオラクル f および g が

m ビットデータ列を n-m ビットランダム数にマッピングし、ランダムオラクル h が n-m ビットデータ列を m ビットランダム数にマッピングする場合に、そのランダムオラクル f、g および h を用いて、第 1 の通信システムの n ビット鍵と第 2 の通信システムの m ビット鍵との間で変換を行うものとして記載してきた。しかしながら、同様に、異なるランダム関数を、異なるあるいは付加的な関数として用いて、x ビットデータ列を y ビットランダム数にマッピングし、かつ/または y ビットデータ列を x ビットランダム数にマッピングすることができる。

ただし、x あるいは y は n-m あるいは m に等しくすることができる。さらに、第 1 の通信システムの m ビット鍵値を 1 つの鍵、複数の鍵あるいはその一部として用いることができ、第 2 の通信システムの n ビット鍵値を 1 つの鍵、複数の鍵あるいはその一部として用いることができる。たとえば、2G TDMA および 3G システムを用いる例では、その変換は、3G システムの 128 ビット CK と、2G TDMA システムの SMEKE Y および VPMASK のための 584 ビット鍵値との間で行われるが、その変換は、3G システムの CK および IK の 256 ビット鍵値と、2G TDMA システムの

SMEKEYおよびVPMASKのための584ビット鍵値との間で行われることもできるであろう。

【0046】上記の例では、順方向変換は、第1の通信システムのmビット鍵値から第2の通信システムのnビット鍵値へ行われ、第1の通信システムは新しい通信システムに対応し、第2の通信システムは古い通信システムに対応し、 $m < n$ である。しかしながら、実施形態によつては、第1の通信システムを古い通信システムにし、第2の通信システムを新しい通信システムにすることができる。別法では、順方向変換を、ある通信システムの小さいサイズの鍵値から別の通信システムの大きいビットサイズの鍵値への変換にし、逆方向変換を、大きいビットサイズの鍵値から小さいサイズの鍵値への変換にことができる。実施形態によつては、種々の通信システム間の異なるサイズ、さらに大きなサイズ、さらに小さなサイズおよび／または同じサイズの鍵値の変換も可能である。

【0047】さらに、その鍵変換システムを用いて、図5～図10に記載されるシステム間ハンドオフを処理して、ある通信システムからの1つの鍵、複数の鍵あるいはその一部を、別の通信システムの1つの鍵、複数の鍵あるいはその一部に変換することができる。種々の値、入力およびアーキテクチャブロックの種々の表記、参照および特徴描写を用いることは理解されたい。たとえば、鍵変換システムのために記載された機能は、ホーム認証局、ホームロケーションレジスタ（HLR）、ホームMSC、ビジター認証局、ビジターロケーションレジスタ（VLR）および／またはビジターモバイルにおいて実行されることができる。さらに鍵変換システムおよびその一部は、第1および／または第2の通信システムの無線ユニット、基地局、基地局コントローラ、MSC、VLR、HLRあるいは他のサブシステムにおいて実行されることができる。そのシステムおよびその一部、ならびに記載されたアーキテクチャは、その通信システムのユニット内、あるいは異なる場所にある処理回路内に実装されるか、またはその処理回路と一体に実装されることができるか、あるいは特定用途向け集積回路、ソフトウェア駆動処理回路、プログラマブルロジック装置、ファームウェア、ハードウェアあるいは個別の構成部品の他の構成内に実装されることができ、それは、本発明の開示の利点を鑑みて当業者には理解されるであろう。記載されてきた内容は、本発明の原理の応用形態を例示しているにすぎない。当業者であれば、本明細書に図示および記載される典型的な応用形態に厳密

に従うことなく、かつ本発明の精神および範囲から逸脱することなく、本発明に対するこれらの、および種々の他の変更形態、構成および方法を実施することができることは容易に理解するであろう。

【0048】

【発明の効果】上記のように、本発明によれば、第1の通信システムの第1の鍵値を第2の通信システムの第2の鍵値に、決定論的に、かつ可逆的に変換するための鍵変換システムを実現することができる。

10 【図面の簡単な説明】

【図1】本発明の原理にしたがった鍵変換システムを用いることができる無線通信システムの全体図である。

【図2】従来の2Gの移動体のためのグローバルシステム（GSM）ネットワークの基本的な構成要素および2G GSMネットワークにおいて伝送されるセキュリティメッセージを示すブロック図である。

【図3】従来の3G UMTSネットワークの基本的な構成要素および3G UTMSネットワークにおいて伝送されるメッセージを示すブロック図である。

20 【図4】従来の2G IS-41ネットワークの基本的な構成要素および従来の2G IS-41ネットワークにおいて伝送されるメッセージを示すブロック図である。

【図5】ユーザが、2G TDMAネットワークから包括的な3Gネットワークに如何にローミングするかを示すブロック図である。

【図6】ユーザが、包括的な3Gネットワークから2G TDMAネットワークに如何にローミングするかを示すブロック図である。

30 【図7】ユーザが、2G CDMAネットワークから包括的な3Gネットワークに如何にローミングするかを示すブロック図である。

【図8】ユーザが、包括的な3Gネットワークから2G CDMAネットワークに如何にローミングするかを示すブロック図である。

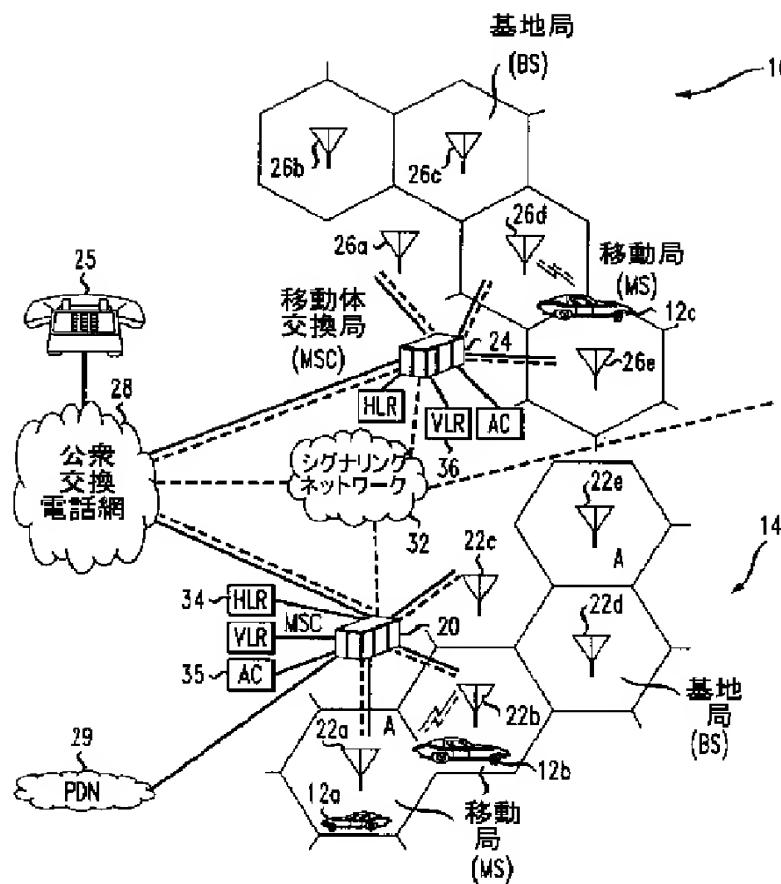
【図9】ユーザが、2G GSMネットワークから包括的な3Gネットワークに如何にローミングするかを示すブロック図である。

40 【図10】ユーザが、包括的な3Gネットワークから2G GSMネットワークに如何にローミングするかを示すブロック図である。

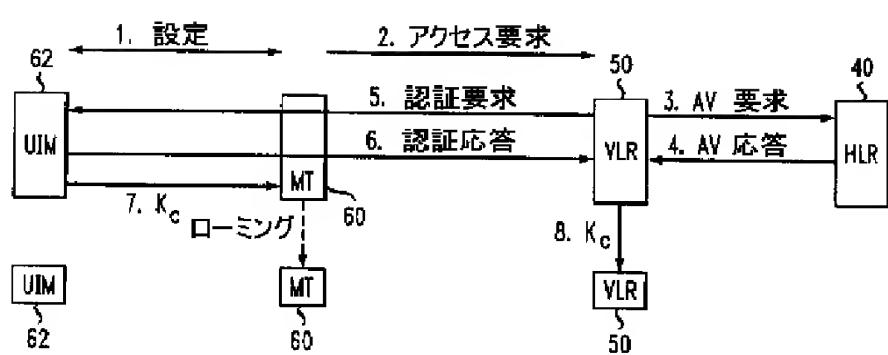
【図11】本発明の原理にしたがった鍵変換システムのための順方向変換の一実施形態の流れ図である。

【図12】本発明の原理にしたがった鍵変換システムのための逆方向変換の一実施形態の流れ図である。

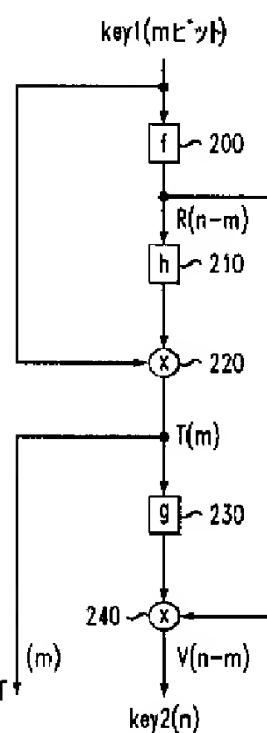
【図1】



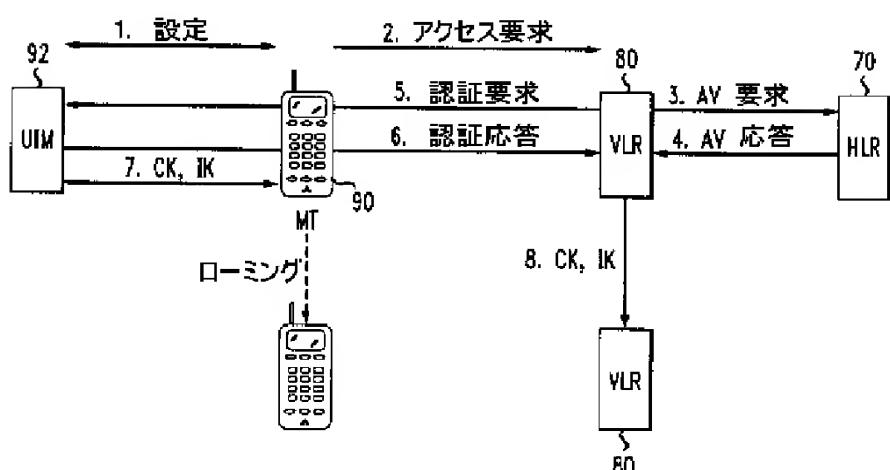
【図2】



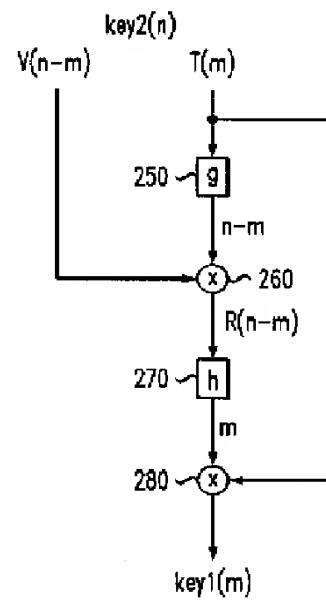
【図11】



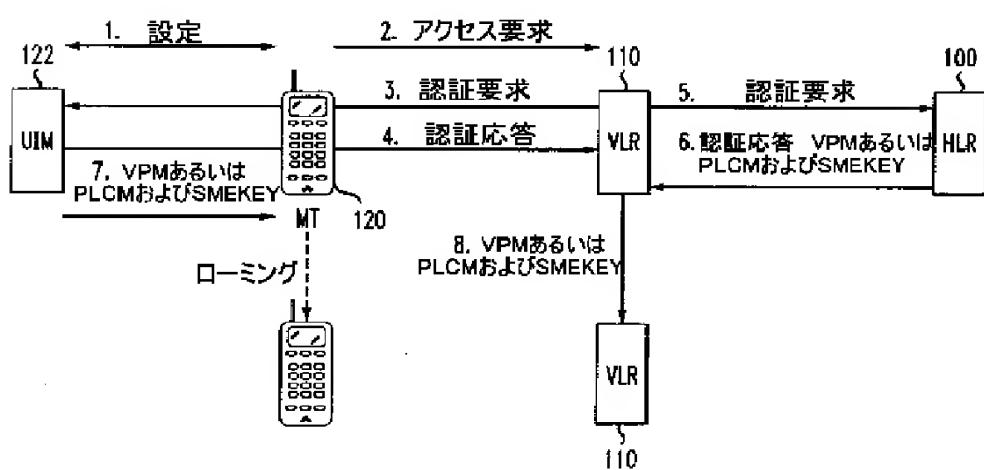
【図3】



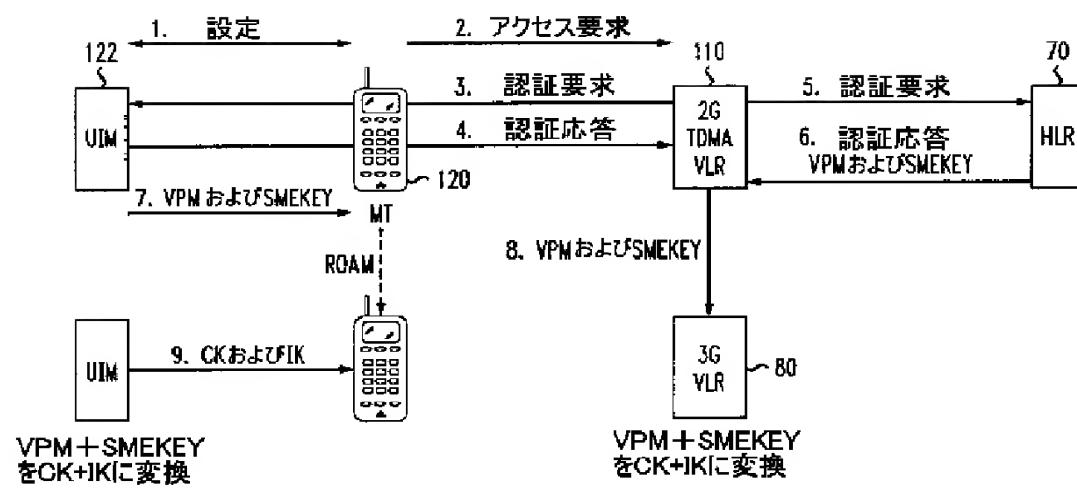
【図12】



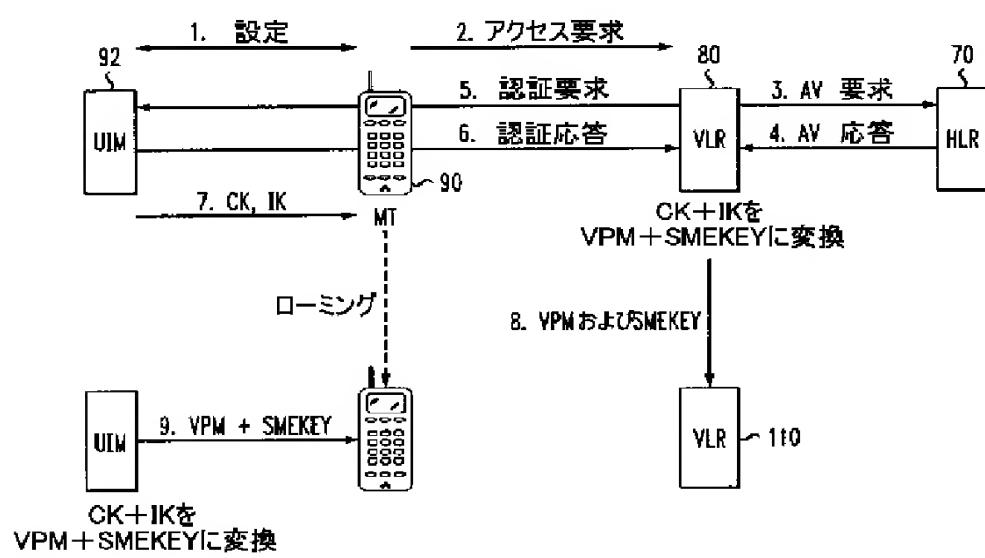
【図4】



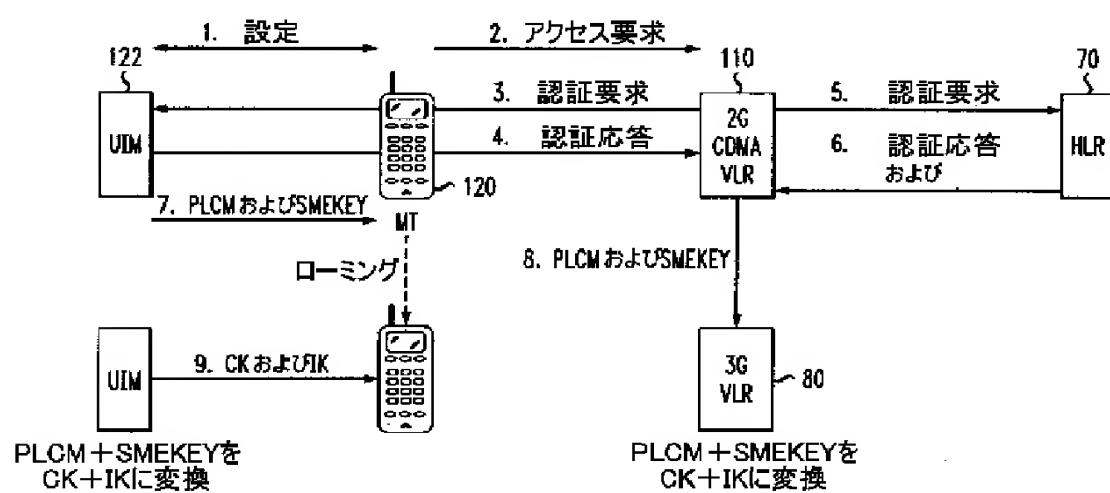
【図5】



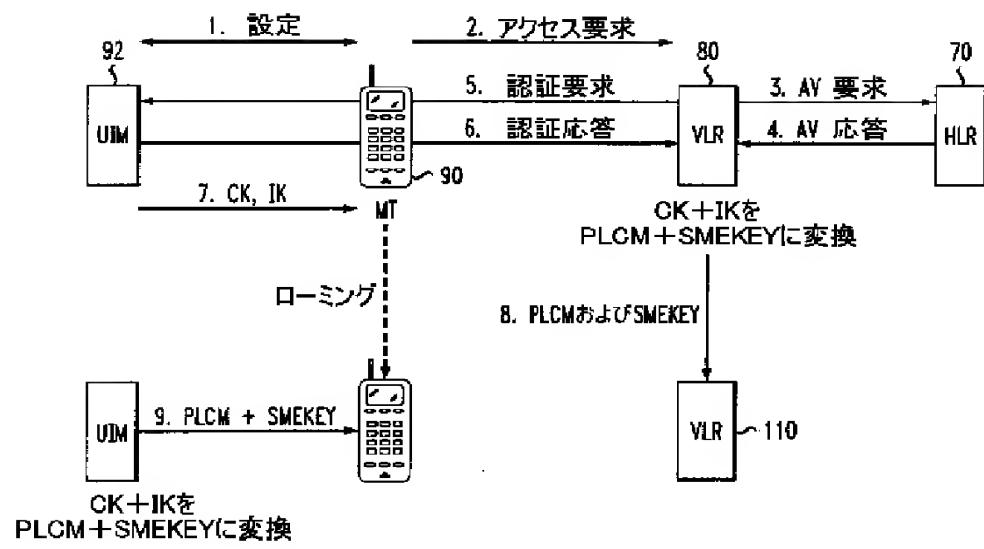
【図6】



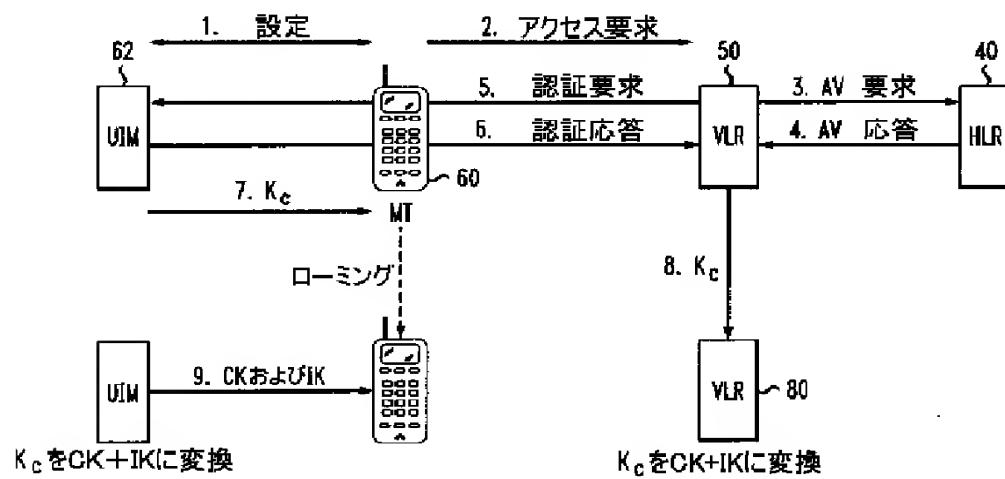
【図7】



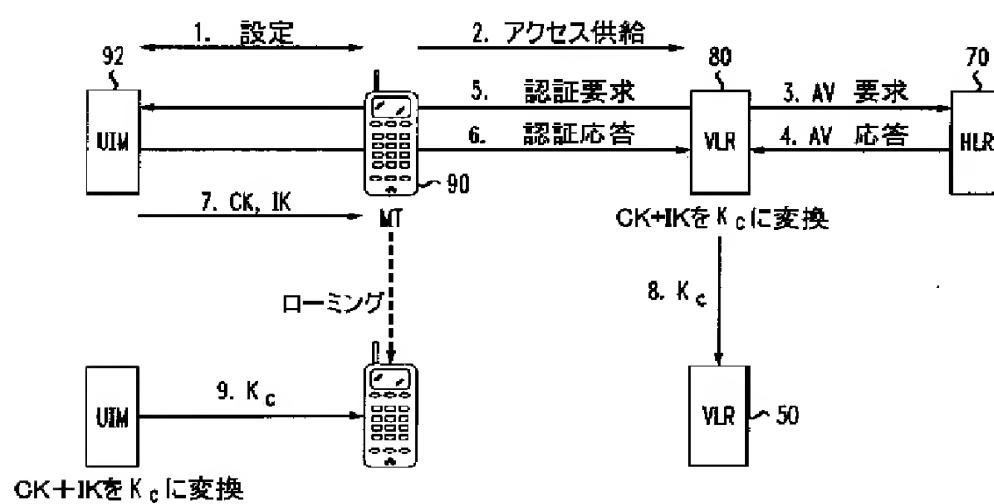
【図8】



【図9】



【図10】



フロントページの続き

F ターム(参考) 5J104 AA01 AA16 BA06 JA04 NA02
NA12 PA02
5K067 AA30 AA32 DD17 DD24 DD57
EE02 EE10 EE16 HH11 HH21
HH23 HH36 JJ31

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成17年7月7日(2005.7.7)

【公開番号】特開2002-232418(P2002-232418A)

【公開日】平成14年8月16日(2002.8.16)

【出願番号】特願2001-376564(P2001-376564)

【国際特許分類第7版】

H 04 L 9/16

H 04 Q 7/38

【F I】

H 04 L 9/00 6 4 3

H 04 B 7/26 1 0 9 S

【手続補正書】

【提出日】平成16年10月26日(2004.10.26)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

第1の通信システムのための第1の鍵値(KEY1)を第2の通信システムのための第2の鍵値(KEY2)に変換する方法であって、

第1のランダム関数(f)を用いて前記第1の鍵値(KEY1)の少なくとも一部から第1の中間値(R)を生成するステップと、

第2の値を生成するために、前記第1の中間値(R)の少なくとも一部を第2のランダム関数(h)に与えるステップと、

第2の中間値(T)を生成するために、前記第1の鍵値(KEY1)の少なくとも一部と、前記第2の値の少なくとも一部とについての排他的論理和を実行するステップと、

第3の値を生成するために、前記第2の中間値(T)の少なくとも一部を第3のランダム関数(g)に与えるステップと、

前記第3の値の少なくとも一部と、前記第1の中間値(R)の少なくとも一部とについての排他的論理和を実行することにより、前記第2の鍵値(KEY2)の少なくとも第1の部分を生成するステップとを含むことを特徴とする方法。

【請求項2】

前記第2の鍵値(KEY2)の少なくとも第2の部分として、前記第2の中間値(T)の少なくとも一部を生成することを特徴とする請求項1に記載の方法。

【請求項3】

前記第1の中間値(R)を生成する前記ステップは、

n-mビットの前記第1の中間値(R)を生成するために、mビットの前記第1の鍵値(KEY1)を第1のランダム関数(f)に与えるステップを含むことを特徴とする請求項1に記載の方法。

【請求項4】

前記第1の中間値(R)の少なくとも一部を第2のランダム関数(h)に与える前記ステップと、前記第1の鍵値(KEY1)の少なくとも一部と前記第2の値の少なくとも一部とについての排他的論理和を実行する前記ステップとは、

mビットの第2の値を生成するために、前記n-mビットの第1の中間値(R)を第2のランダム関数(h)に与えるステップと、

mビットを有する前記第2の中間値(T)を生成するために、前記mビットの第1の鍵値(KEY1)と前記mビットの第2の値とについての排他的論理和を実行するステップとを含むことを特徴とする請求項3に記載の方法。

【請求項5】

前記第2の中間値(T)の少なくとも一部を第3のランダム関数(g)に与える前記ステップと、前記第2の鍵値(KEY2)の少なくとも第1の部分を生成する前記ステップとは、

n-mビットの第3の値を生成するために、前記mビットの第2の中間値(T)を第3のランダム関数(g)に与えるステップと、

前記第2の鍵値(KEY2)のn-mビットの部分(V)を生成するために、前記n-mビットの第3の値と、前記n-mビットの第1の中間値(R)とについての排他的論理和を実行するステップとを含むことを特徴とする請求項4に記載の方法。

【請求項6】

nビットを有する前記第2の鍵値(KEY2)のmビットの第2の部分として、前記mビットの第2の中間値(T)を与えるステップを含むことを特徴とする請求項5に記載の方法。

【請求項7】

前記第3の値を生成するために、前記第2の鍵値(KEY2)の前記第2の部分(T)を、前記第3のランダム関数(g)に与えるステップと、

前記第2の鍵値(KEY2)の前記第1の部分(V)と、前記第3の値との排他的論理和をとることにより、前記第1の中間値(R)を生成するステップとを含むことを特徴とする請求項2に記載の方法。

【請求項8】

前記第1の中間値(R)から前記第2の値を生成するために、前記第2のランダム関数(h)を用いるステップと、

前記第2の値と、前記第2の鍵値(KEY2)の前記第2の部分(T)との排他的論理和をとることにより、前記第1の鍵値の少なくとも一部を生成するステップとをさらに含むことを特徴とする請求項7に記載の方法。

【請求項9】

第1の通信システムのための第1の鍵値(KEY1)を第2の通信システムのための第2の鍵値(KEY2)に変換するための鍵変換システムであって、

第1のランダム関数(f)を用いて、前記第1の鍵値(KEY1)の少なくとも一部から第1の中間値(R)を生成するように構成され、前記第1の中間値(R)の少なくとも一部を第2のランダム関数(h)に与えて第2の値を生成するように構成され、前記第1の鍵値(KEY1)の少なくとも一部と前記第2の値の少なくとも一部とについての排他的論理和を実行して第2の中間値(T)を生成するように構成され、前記第2の中間値(T)の少なくとも一部を第3のランダム関数(g)に与えて第3の値を生成するように構成され、さらに、前記第3の値の少なくとも一部と前記第1の中間値(R)の少なくとも一部との排他的論理和をとることにより前記第2の鍵値(KEY2)の少なくとも第1の部分を生成するように構成される処理回路を含むことを特徴とする鍵変換システム。

【請求項10】

前記処理回路はさらに、前記第2の鍵値(KEY2)の少なくとも第2の部分として、前記第2の中間値(T)の少なくとも一部を生成するように構成されることを特徴とする請求項9に記載のシステム。



US 20020071558A1

(19) **United States**

(12) Patent Application Publication
Patel

(10) Pub. No.: US 2002/0071558 A1

(43) Pub. Date: Jun. 13, 2002

(54) KEY CONVERSION SYSTEM AND METHOD

(76) Inventor: **Sarvar Patel**, Montville, NJ (US)

**Correspondence Address:
Docket Administrator (Rm. 3C-512)
Lucent Technologies Inc.
600 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636 (US)**

(21) Appl. No.: 09/734,148

(22) Filed: **Dec. 11, 2000**

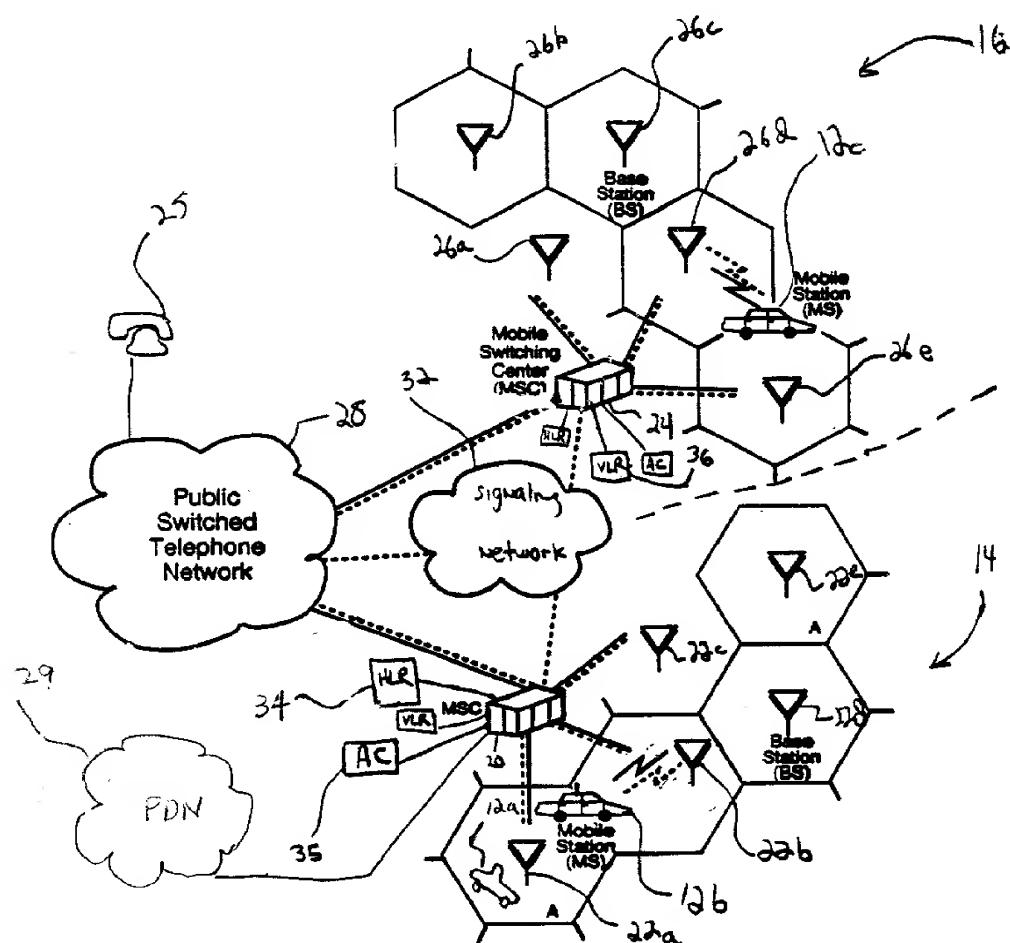
Publication Classification

(51) Int. Cl.⁷ H04K 1/00
(52) U.S. Cl. 380/270; 380/277

(57) **ABSTRACT**

The present invention is a key conversion system for deterministically and reversibly converting a first key value of a first communications system into a second key value of a second communication system. For example, the key conversion system generates a first intermediate value from at least a portion of the first key value using a first random function. At least a portion of the first intermediate value is

provided to a second random function to produce a second value. An exclusive-or is performed on at least a portion of the first key value and at least a portion of the second value to generate a second intermediate value. At least a portion of the second intermediate value is provided to a third random function to produce a third value. By performing an exclusive-or on at least a portion of the third value and at least a portion of the first intermediate value, the key conversion system produces at least a first portion of the second key value, and at least a second portion of the second key value is produced as the second intermediate value. The key conversion system is reversible or bi-directional in that, if the wireless unit is handed off back to the first communications system, the second key value of the second communications system is converted back to the first key value of the first communications system. For example, the key conversion system provides the at least second portion of the second key value to the third random function to produce the third value. The first intermediate value is generated by performing an exclusive-or on the first portion of the second key value and the third value. Using the second random function, the key conversion system generates the second value from the first intermediate value and produces at least a portion of the first key by performing an exclusive-or on the second value and the second portion of the second key value.



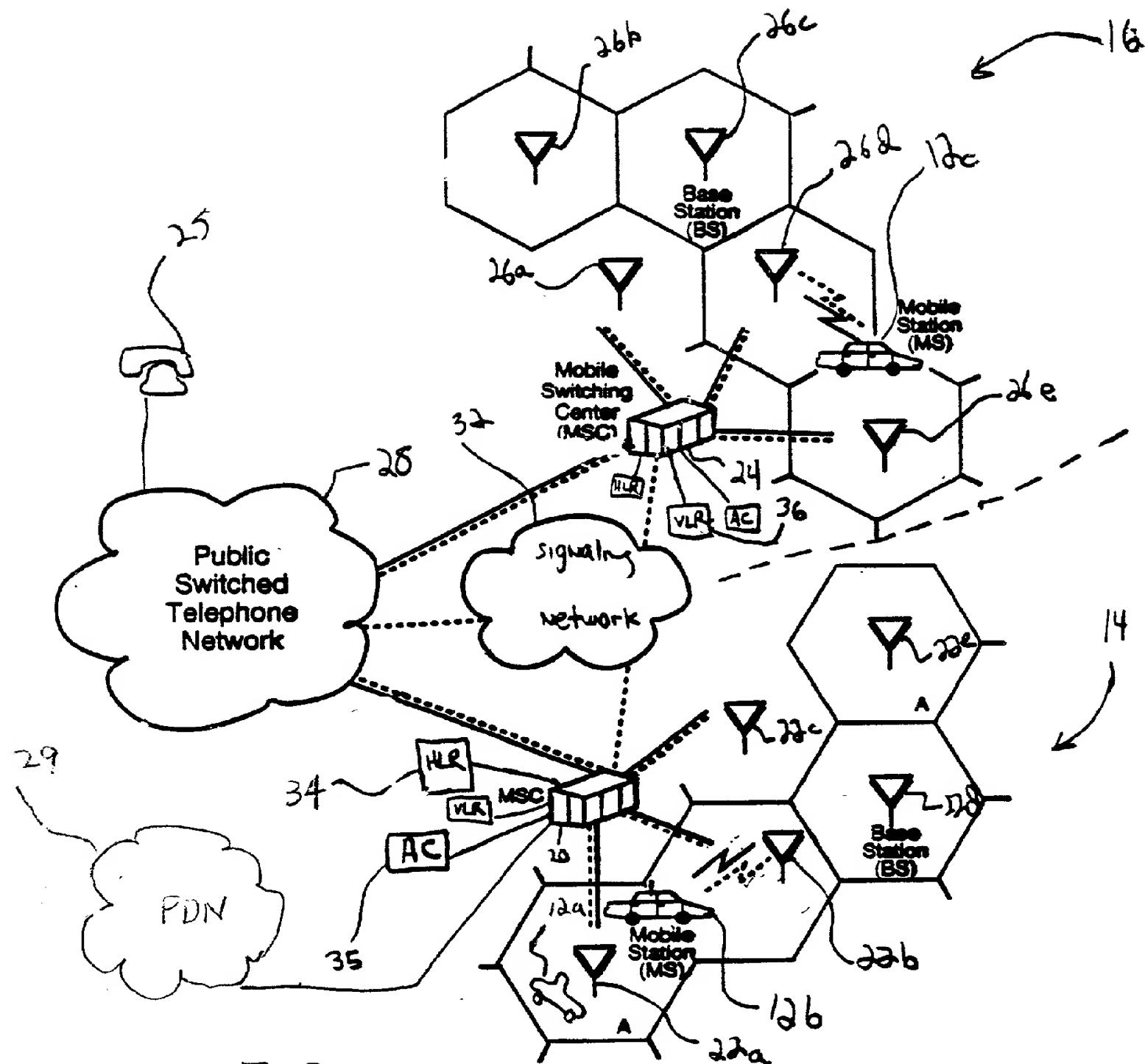
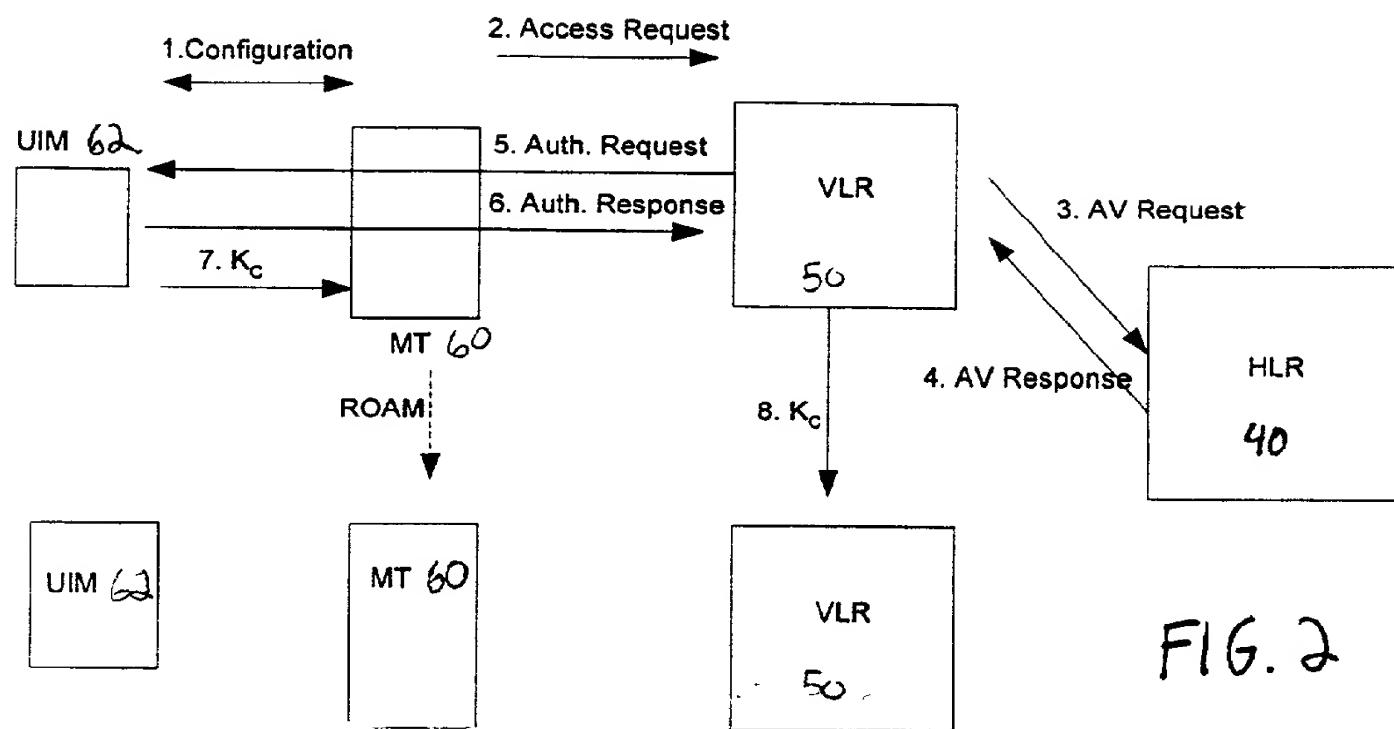


FIG. I



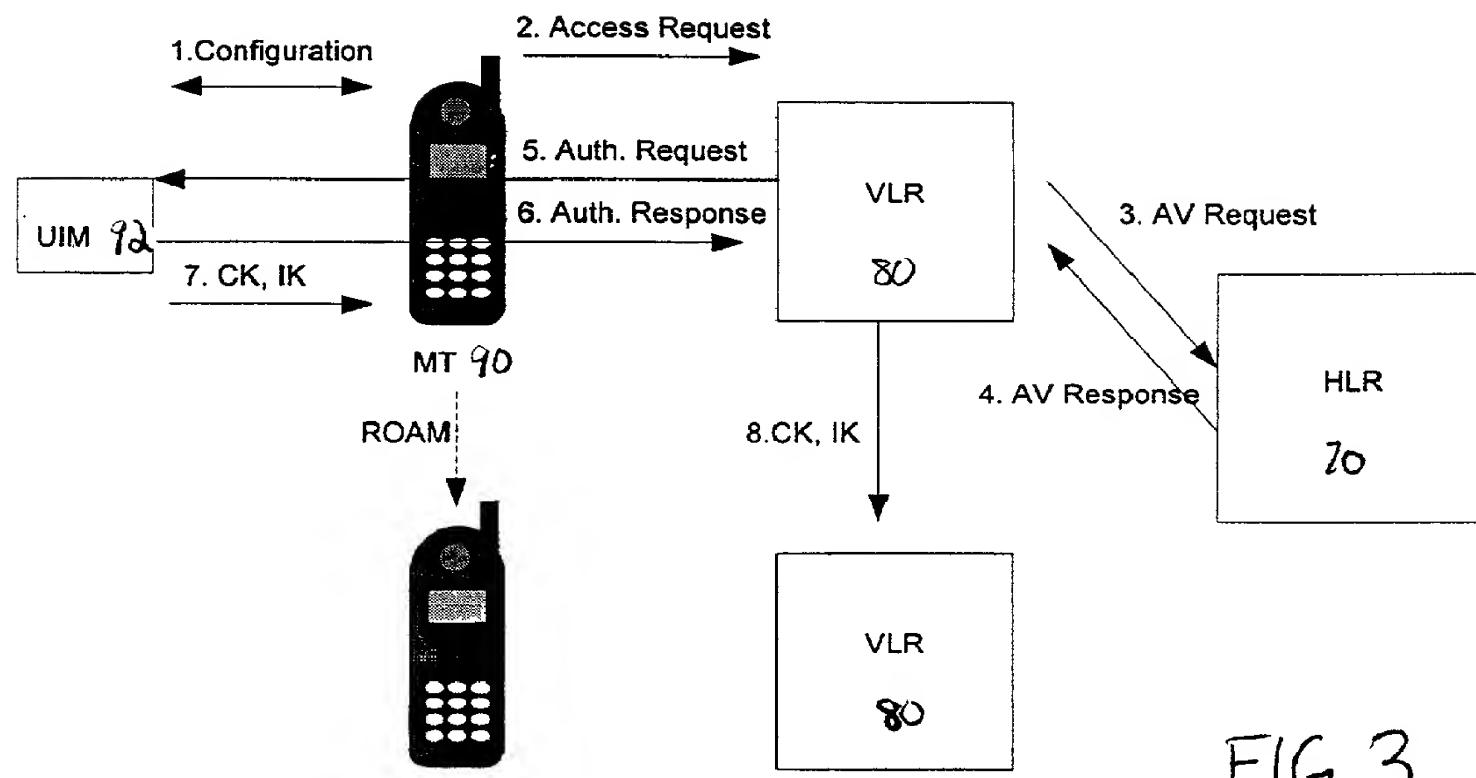


FIG. 3

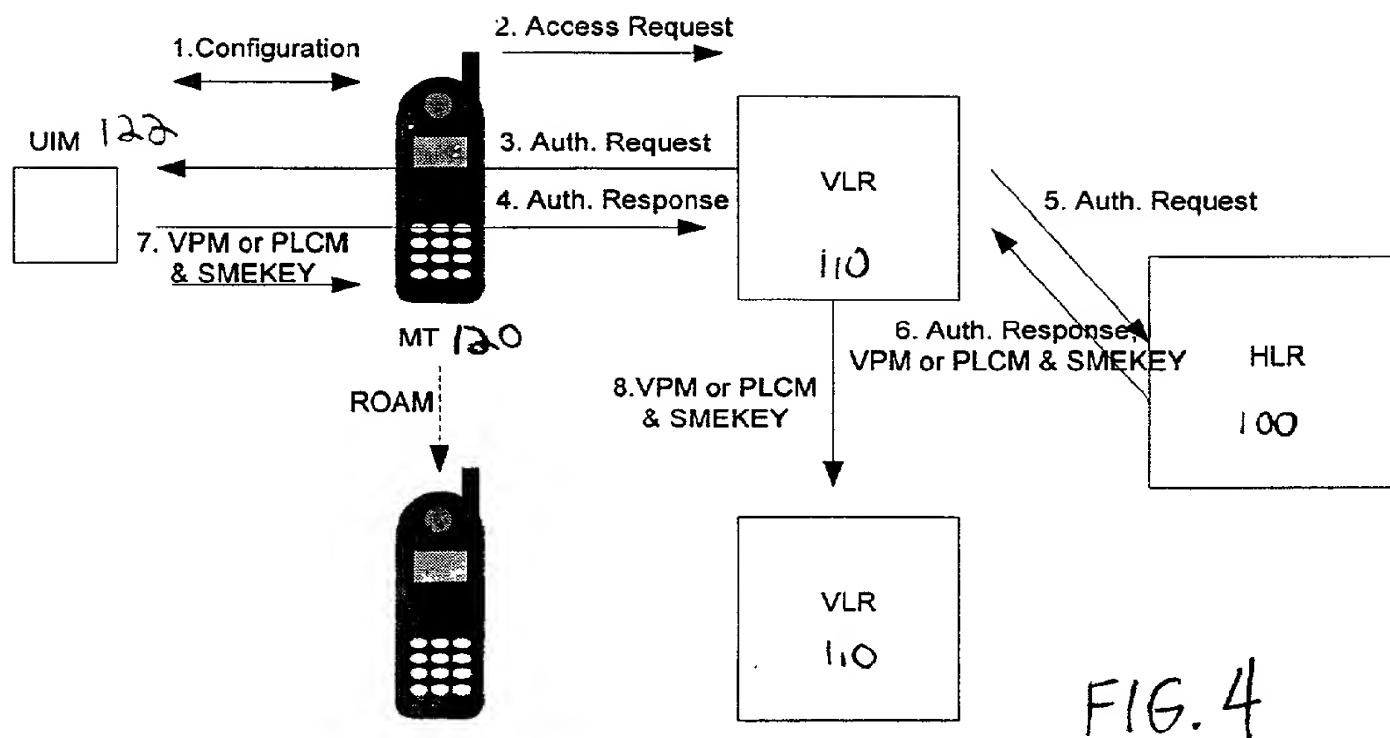
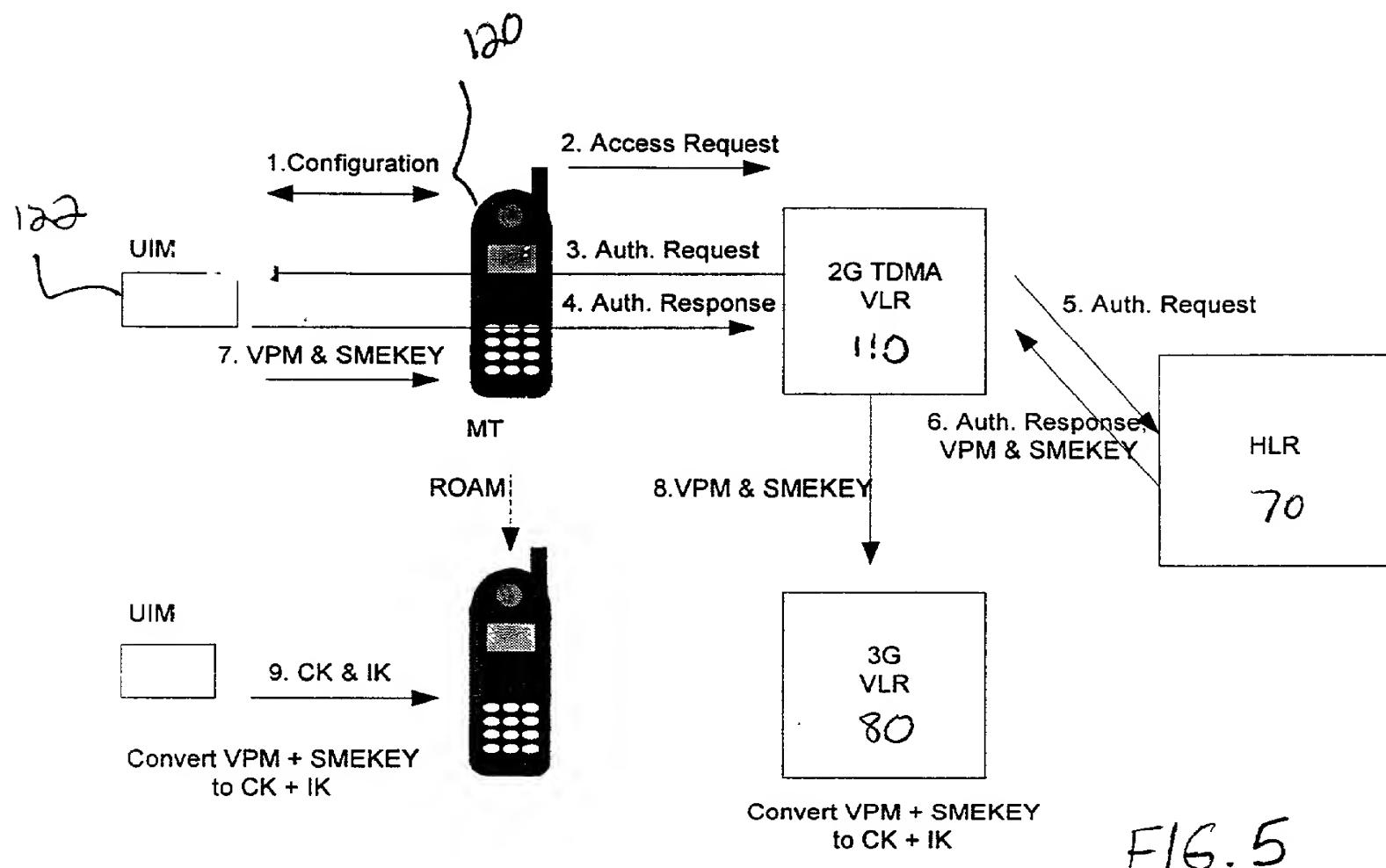


FIG. 4



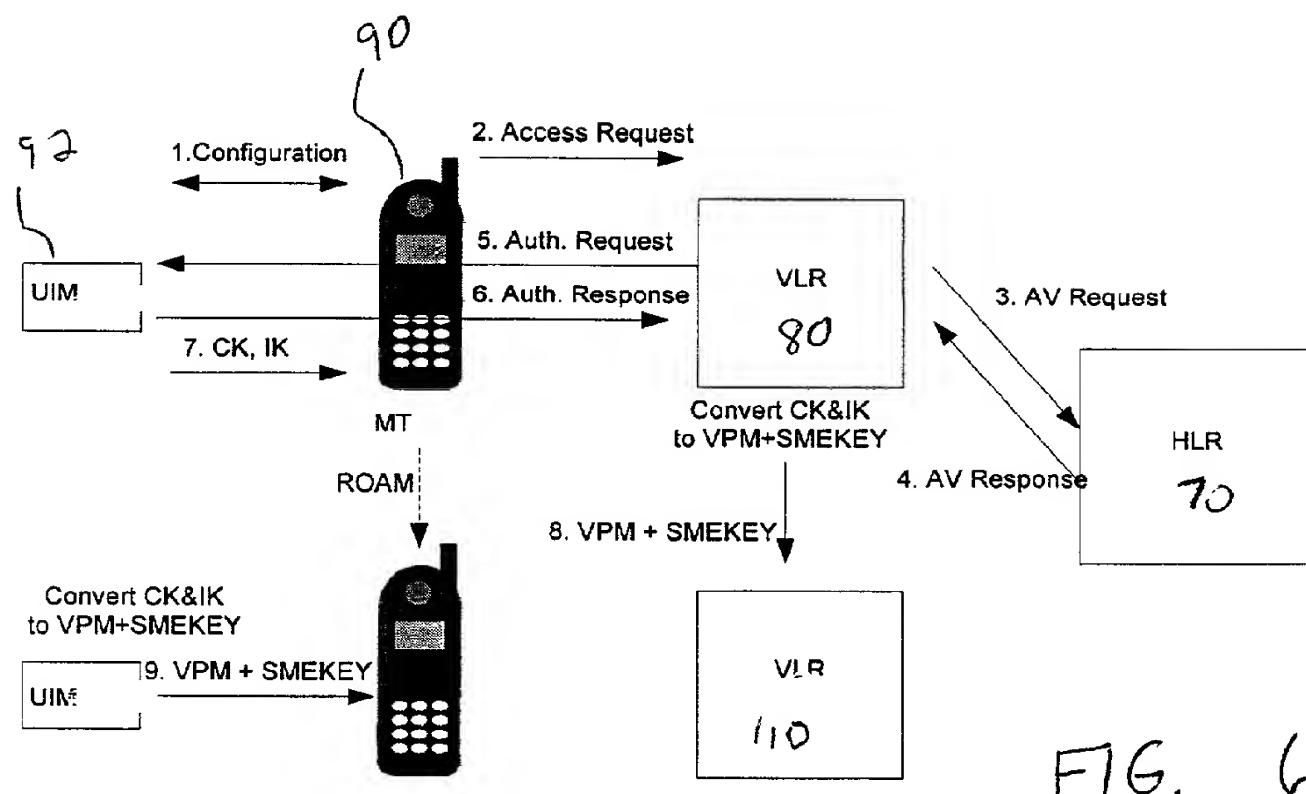


FIG. 6

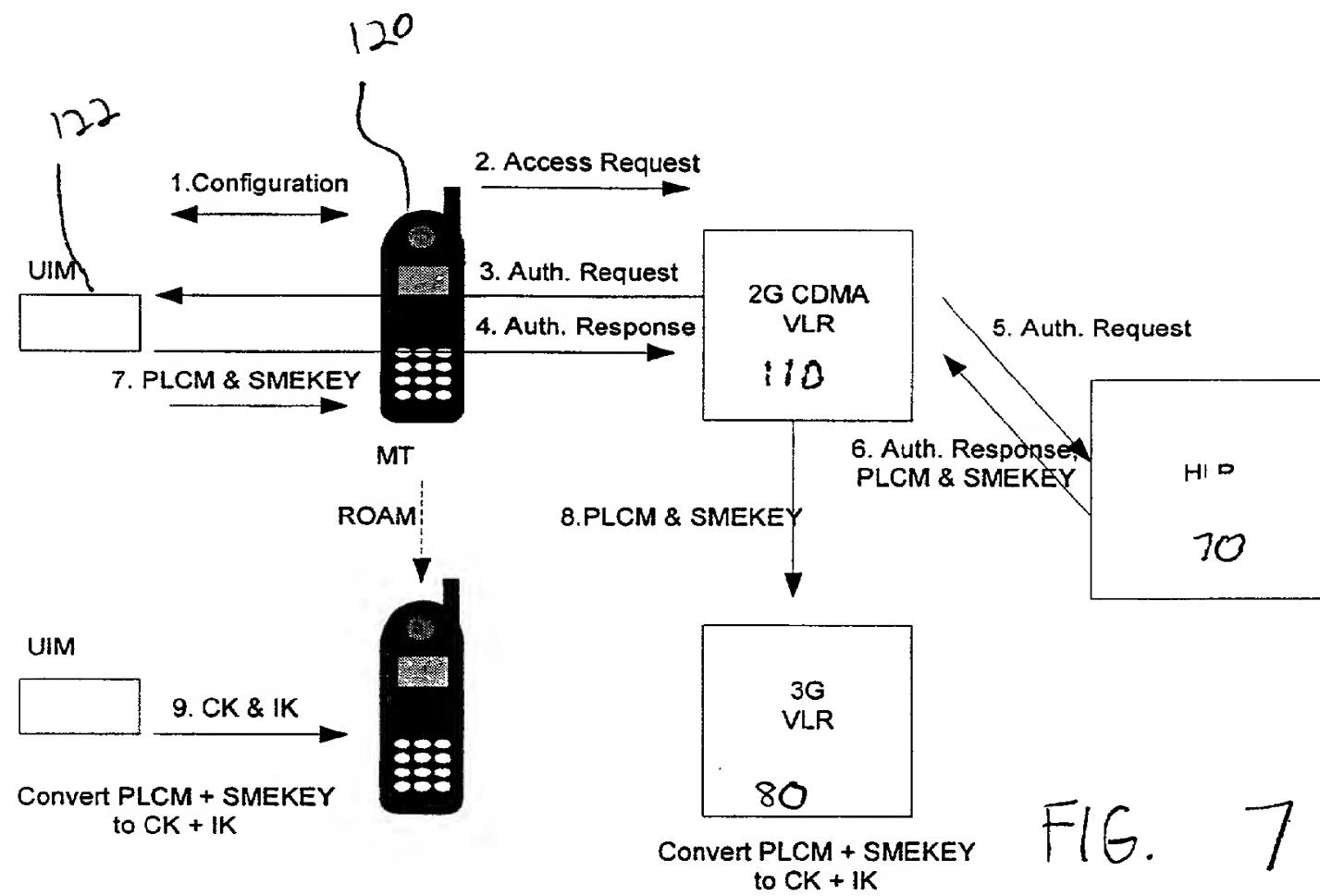


FIG. 7

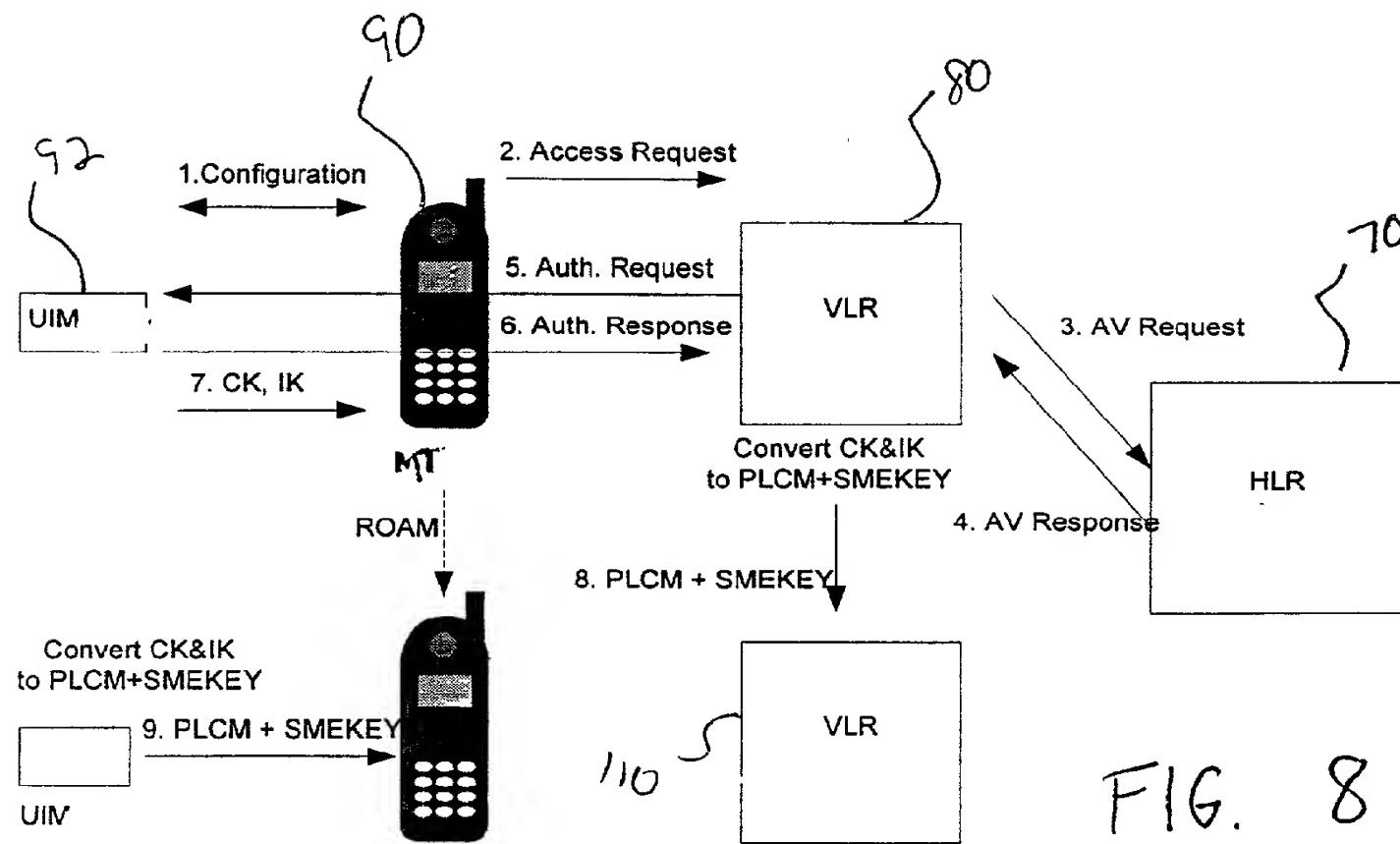


FIG. 8

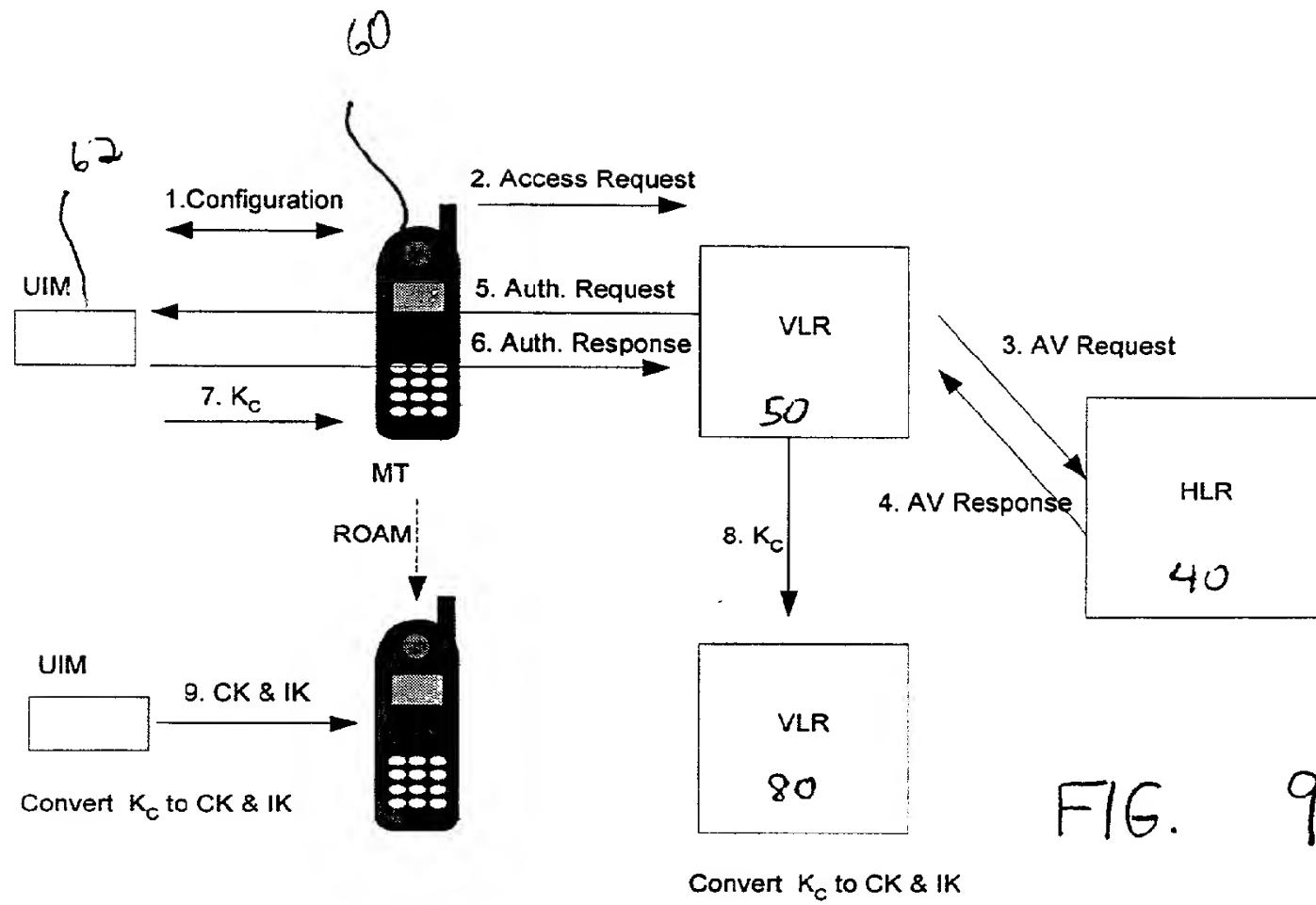
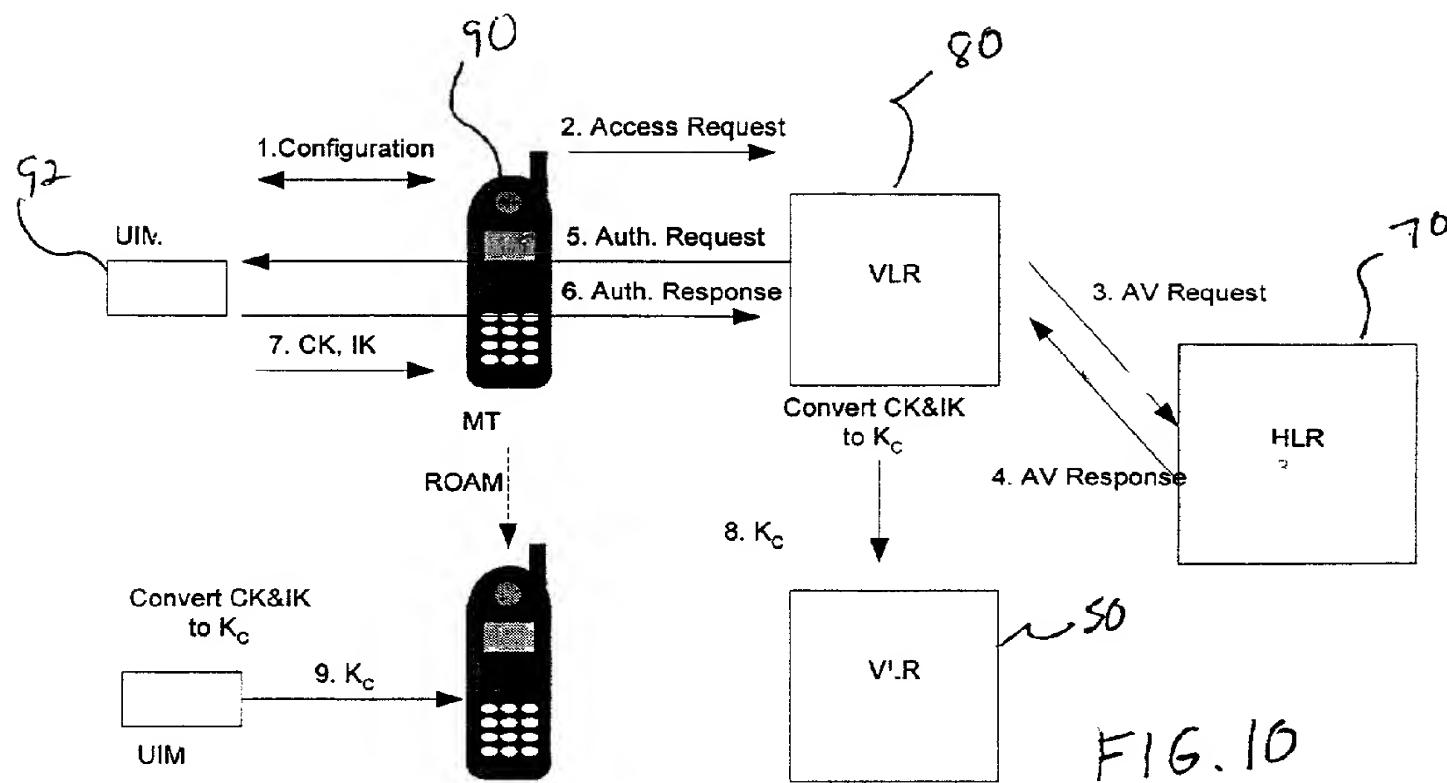
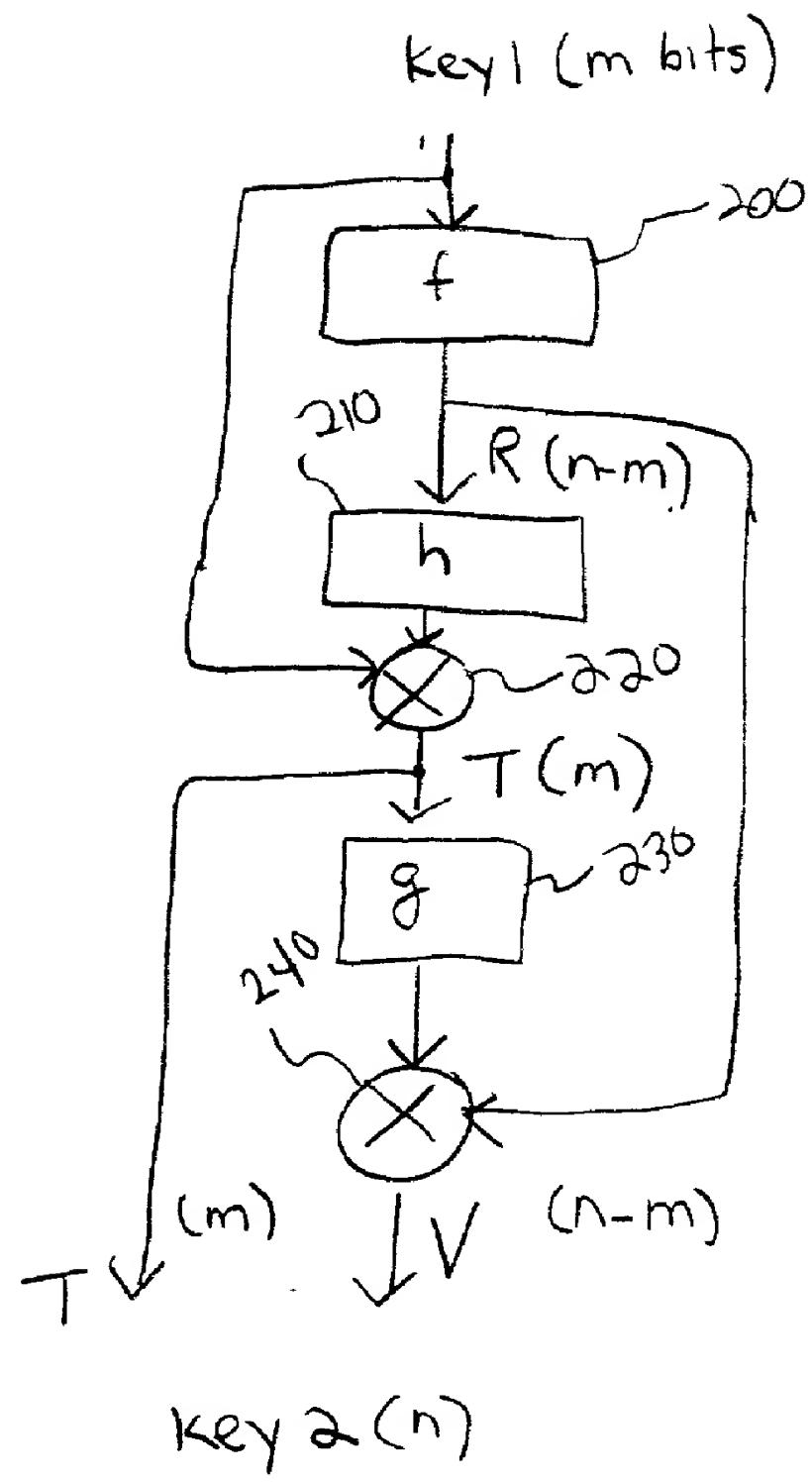


FIG. 9

Convert K_c to CK & IK





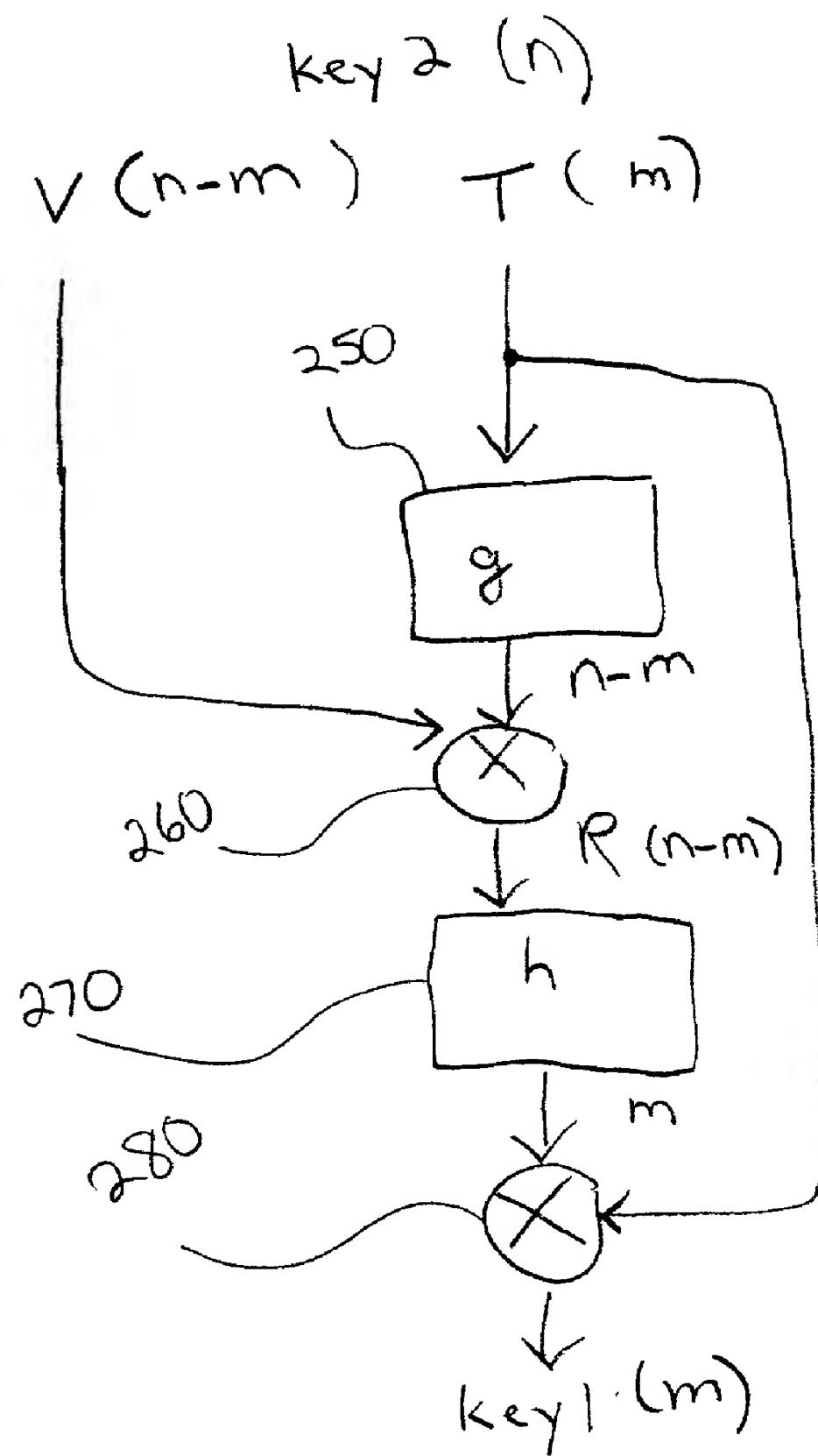


FIG. 12

KEY CONVERSION SYSTEM AND METHOD

BACKGROUND OF THE INVENTION

[0001] 1. Field of The Invention

[0002] The present invention relates to communications; more specifically, the conversion of keys for first and second communications systems as the wireless unit roams between the first and second communications systems.

[0003] 2. Description of Related Art

[0004] **FIG. 1** depicts a schematic diagram of first and second wireless communications systems which provide wireless communications service to wireless units (e.g., wireless units 12a-c) that are situated within the geographic regions 14 and 16, respectively. A Mobile Switching Center (e.g. MSCs 20 and 24) is responsible for, among other things, establishing and maintaining calls between the wireless units, calls between a wireless unit and a wireline unit (e.g., wireline unit 25), and/or connections between a wireless unit and a packet data network (PDN), such as the internet. As such, the MSC interconnects the wireless units within its geographic region with a public switched telephone network (PSTN) 28 and/or a packet data network (PDN) 29. The geographic area serviced by the MSC is divided into spatially distinct areas called "cells." As depicted in **FIG. 1**, each cell is schematically represented by one hexagon in a honeycomb pattern; in practice, however, each cell has an irregular shape that depends on the topography of the terrain surrounding the cell.

[0005] Typically, each cell contains a base station (e.g. base stations 22a-e and 26a-e), which comprises the radios and antennas that the base station uses to communicate with the wireless units in that cell. The base stations also comprise the transmission equipment that the base station uses to communicate with the MSC in the geographic area. For example, MSC 20 is connected to the base stations 22a-e in the geographic area 14, and an MSC 24 is connected to the base stations 26a-e in the geographic region 16. Within a geographic region, the MSC switches calls between base stations in real time as the wireless unit moves between cells, referred to as call handoff. Depending on the embodiment, a base station controller (BSC) can be a separate base station controller (BSC) (not shown) connected to several base stations or located at each base station which administers the radio resources for the base stations and relays information to the MSC.

[0006] The MSCs 20 and 24 use a signaling network 32, such as a signaling network conforming to the standard identified as TIA/EIA-41-D entitled "Cellular Radiotelecommunications Intersystem Operations," December 1997 ("IS-41"), which enables the exchange of information about the wireless units which are roaming within the respective geographic areas 14 and 16. For example, a wireless unit 12a is roaming when the wireless unit 12a leaves the geographic area 14 of the MSC 20 to which it was originally assigned (e.g. home MSC). To ensure that a roaming wireless unit can receive a call, the roaming wireless unit 12a registers with the MSC 24 in which it presently resides (e.g., the visitor MSC) by notifying the visitor MSC 24 of its presence. Once a roaming wireless unit 12a is identified by a visitor MSC 24, the visitor MSC 24 sends a registration request to the home MSC 20 over the signaling network 32, and the home

MSC 20 updates a database 34, referred to as the home location register (HLR), with the identification of the visitor MSC 24, thereby providing the location of the roaming wireless unit 12a to the home MSC 20.

[0007] After a roaming wireless unit is authenticated, the home MSC 20 provides to the visitor MSC 24 a customer profile which indicates the features available to the roaming wireless unit, such as call waiting, caller id, call forwarding, three-way calling, and international dialing access. Upon receiving the customer profile, the visitor MSC 24 updates a database 36, referred to as the visitor location register (VLR), to provide the same features as the home MSC 20. The KLR, VLR and/or the authentication center (AC) can be co-located at the MSC or remotely accessed.

[0008] If a wireless unit is roaming between wireless communications systems using different wireless communications standards, providing the wireless unit with the same features and services in the different wireless communications systems is complex if even feasible. There are currently different wireless communication standards utilized in the U.S., Europe, and Japan. The U.S. currently utilizes two major wireless communications systems with differing standards. The first system is a time division multiple access system (TDMA) and is governed by the standard known as IS-136, the second system is a code division multiple access (CDMA) system governed by the standard known as IS-95. Both communication systems use the standard known as IS-41 for intersystem messaging, which defines the authentication procedure.

[0009] In TDMA, users share a frequency band, each user's speech is stored, compressed and transmitted as a quick packet, using controlled time slots to distinguish them, hence the phrase "time division". At the receiver, the packet is decompressed. In the IS-136 protocol, three users share a given carrier frequency. In contrast, CDMA uses a unique code to "spread" the signal across the wide area of the spectrum (hence the alternative name -spread spectrum), and the receiver uses the same code to recover the signal from the noise. A very robust and secure channel can be established, even for an extremely low-power signal. Further, by using different codes, a number of different channels can simultaneously share the same carrier signal without interfering with each other. Both CDMA and TDMA systems are defined for a Second Generation (2G) and Third Generation (3G) phases with differing requirements for user information privacy or confidentiality.

[0010] Europe utilizes the Global System for Mobiles (GSM) network as defined by the European Telecommunications Standard Institute (ETSI). GSM is a TDMA standard, with 8 users per carrier frequency. The speech is taken in 20 msec windows, which are sampled, processed, and compressed. GSM is transmitted on a 900 MHz carrier. There is an alternative system operating at 1.8 GHz (DCS 1800), providing additional capacity, and is often viewed as more of a personal communication system (PCS) than a cellular system. In a similar way, the U.S. has also implemented DCS-1900, another GSM system operating on the different carrier of 1.9 GHz. Personal Digital Cellular (PDC) is the Japanese standard, previously known as JDC (Japanese Digital Cellular). PDC is a TDMA standard similar to the U.S. standard known as IS-54 protocol.

[0011] The GSM network utilizes a removable user identification module (UIM) which is a credit card size card

which is owned by a subscriber, who slides the UIM into any GSM handset to transform it into “their” phone. It will ring when their unique phone number is dialed, calls made will be billed to their account; all options and services connect; voice mail can be connected and so on. People with different UIMs can share one “physical” handset, turning it into several “virtual” handsets, one per UIM. Similar to the U.S. systems, the GSM network also permits “roaming”, by which different network operators agree to recognize (and accept) subscribers from other wireless communications systems or networks, as wireless units (or UIMs) move. So, British subscribers can drive through France or Germany and use their GSM wireless unit to make and receive calls (on their same UK number), with as much ease as an American businessman can use a wireless unit in Boston, Miami, or Seattle, within any one of the U.S. wireless communications system. The GSM system is defined as a Second Generation (2G) system.

[0012] The third generation (3G) enhancement of the GSM security scheme is defined in the Universal Mobile Telecommunications Service (UMTS) set of standards, and specifically for the security in the standard identified as 3GPP TS-33.102 “Security Architecture” specifications. This security scheme with slight variations will be used as a basis for the worldwide common security scheme for all 3G communications systems, including UMTS, TDMA, and CDMA.

[0013] The 2G GSM authentication scheme is illustrated in **FIG. 2**. This authentication scheme includes a home location register (HLR) **40**, a visiting location register (VLR) **50**, and a wireless unit or mobile terminal (MT) **60**, which includes a UIM **62**. When the mobile terminal **60** places a call, a request is sent to the home location register **40**, which generates an authentication vector AV, also called “triplet” (RAND, SRES, K_c) from a root key K_i . The triplet includes a random number RAND, a signed response SRES, and a session key K_c . The triplet is provided to the visiting location register **50**, which passes the random number RAND to the mobile terminal **60**. The UIM **62** receives the random number RAND, and utilizing the root key K_i , the random number RAND, and an algorithm A3, calculates a signed response SRES. The UIM **62** also utilizes the root key K_i and the random number RAND, and an algorithm A8 to calculate the session key K_c . The SRES, calculated by the UIM **62**, is returned to the visiting location register **50**, which compares this value from the SRES received from the home location register **40**, in order to authenticate the subscriber using the mobile terminal **30**.

[0014] In the GSM “challenge/response” authentication system, the visiting location register **50** never receives the root key K_i being held by the UIM **32** and the home location register **40**. The VLR **50** also does not need to know the authentication algorithms used by the HLR **40** and UIM **62**. Also, in the GSM authentication scheme, the triplet must be sent for every phone call by the home location register **40**. RAND is 128 bits, SRES is 32 bits, and K_c is 64 bits, which is 224 bits of data for each request, which is a significant data load. The main focus of this description is the 64 bits long K_c session ciphering key which is used for user information confidentiality. When the mobile terminal roams into another serving system while in the call, the session key K_c is forwarded from the old VLR to the new target serving system.

[0015] **FIG. 3** shows the UMTS security scheme which is an enhancement to the 2G GSM scheme. Similar to the GSM scheme, when the mobile terminal **90** places a call, a request is sent to the home location register **70**, which sends an authentication vector—AV to the Visited Location Register (VLR) **80** which contains five elements instead of the three elements of a triplet, and therefore is called “quintuplet”. This vector contains the 128 bit RAND, the 64 bits SRES, the AUTN value which carries the authentication signature of the home network, and two session security keys: the 128 bit ciphering key CK and the 128 bit integrity key IK. These latter two keys, CK and IK, are the focus of this description.

[0016] The vector is provided to the visiting location register **80**, which passes the random number RAND and the AUTN to the mobile terminal **90**. The UIM **92** receives the random number RAND, and utilizing the root key K_i , the random number RAND, and an defined algorithmic functions, validates the AUTN and calculates a signed response SRES. The UIM **92** also utilizes the root key K_i and the random number RAND and defined algorithmic functions to calculate the session keys CK and IK. The SRES, calculated by the UIM **92**, is returned to the visiting location register **80**, which compares this value from the SRES received from the home location register **70** in order to authenticate the subscriber using the mobile terminal **90**. A focus of this description are the 128 bits long session ciphering key CK and 128 bits long session integrity key IK which are used for user information confidentiality and session integrity protection. Once the subscriber is successfully authenticated, the VLR **80** activates the CK and IK received in this authentication vector. If the mobile terminal roams into another serving system while on the call, the CK and IK are sent to the new target serving system.

[0017] The 2G IS-41 authentication scheme, used in U.S. TDMA and CDMA systems, is illustrated in **FIG. 4**. This authentication scheme involves a home location register (HLR) **100**, a visiting location register (VLR) **110**, and a mobile terminal (MT) **120**, which can include a UIM **122**. The root key, known as the A_key, is stored only in the HLR **100** and the UIM **122**. There is a secondary key, known as Shared Secret Data SSD, which is sent to the VLR **110** during roaming. SSD is generated from the A_key using a cryptographic algorithm. The procedure for generating the SSD is described elsewhere and is known to those skilled in the art. When the MT **120** roams to a visiting network, the VLR **110** sends an authentication request to the HLR **100**, which responds by sending that subscriber’s SSD. Once the VLR **110** has the SSD, it can authenticate the MT **120** independently of the HLR **100**, or with the assistance of the HLR **100** as is known to those skilled in the art. The VLR **110** sends a random number RAND to the UIM **122** via the MT **120**, and the UIM **122** calculates the authentication response (AUTHR) using RAND and the stored value of SSD in UIM **122**. AUTHR is returned to the VLR **110**, which checks it against the value of AUTHR that it has independently calculated in the same manner. If the two AUTHR values match, the MT **120** is declared valid. This process repeats when the wireless unit attempts to access the system, for instance, to initiate a call, or to answer a page when the call is received.

[0018] In these cases, the session security keys are also generated. To generate session security keys, the internal state of the computation algorithm is preserved after the

authentication calculation. Several session security keys are then calculated by the UIM **122** and the VLR **110** using the current value of SSD. Specifically, the 520 bits Voice Privacy Mask (VPM) is computed, which is used for concealing the TDMA speech data throughout the call. This VPM is derived at the beginning of the call by the UIM and VLR, and, if the mobile roams into another serving system during the call, the VPM is sent to the new serving system by the VLR. When the call is concluded, the VPM is erased by both the UIM and the serving VLR. Likewise, the 64 bits Signaling Message Encryption Key (SMEKEY) is computed, which is used for encrypting the TDMA signaling information throughout the call. This SMEKEY is derived at the beginning of the call by the UIM and VLR, and, if the mobile roams into another serving system during the call, the SMEKEY is sent to the new serving system by the VLR. When the call is concluded, the SMEKEY is erased by both the UIM and the serving VLR.

[0019] The 2G CDMA scheme uses a similar method of key distribution, except, instead of the 520 bits VPM, it is using the 42 Least Significant Bits (LSB) of the VPM as a seed into the Private Long Code Mask (PLCM). This PLCM is used as an additional scrambling mask for the information before its spreading. The 42-bit PLCM is consistent throughout the call and is sent to the new serving system by the VLR if the mobile roams into another serving system. The SMEKEY is used in the same way as in the TDMA based scheme.

[0020] The IS-41 3G security scheme uses the UMTS security scheme, which is based on the delivery of the 128-bits ciphering key CK and 128-bits integrity key IK to the visited system VLR, while the same keys are computed by the UIM.

[0021] Key conversions as a wireless unit roams between communications systems should be performed in a way that even if lower security of 2G schemes and algorithms is compromised and partial keys are recovered by the intruder, the 3G session keys would still maintain the same level of security. Such conversions will allow a subscriber to “roam globally” maintaining the security of communications data and integrity of communications session.

SUMMARY OF THE INVENTION

[0022] The present invention is a key conversion system for deterministically and reversibly converting a first key value of a first communications system into a second key value of a second communication system. For example, the key conversion system generates a first intermediate value from at least a portion of the first key value using a first random function. At least a portion of the first intermediate value is provided to a second random function to produce a second value. An exclusive-or is performed on at least a portion of the first key value and at least a portion of the second value to generate a second intermediate value. At least a portion of the second intermediate value is provided to a third random function to produce a third value. By performing an exclusive-or on at least a portion of the third value and at least a portion of the first intermediate value, the key conversion system produces at least a first portion of the second key value, and at least a second portion of the second key value is produced as the second intermediate value. The key conversion system is deterministic in that, given a first

key value, a wireless unit and the wireless communications system will determine the same second key value without requiring an exchange of information.

[0023] The key conversion system is reversible or bi-directional in that, if the wireless unit is handed off back to the first communications system, the second key value of the second communications system is converted back to the first key value of the first communications system. For example, the key conversion system provides the at least second portion of the second key value to the third random function to produce the third value. The first intermediate value is generated by performing an exclusive-or on the first portion of the second key value and the third value. Using the second random function, the key conversion system generates the second value from the first intermediate value and produces at least a portion of the first key by performing an exclusive-or on the second value and the second portion of the second key value. The key conversion system provides improved security because even if almost all of the second key value is known, the first key value cannot easily be recovered. Similarly, if almost all of the first key value is known, the second key value is not easily recovered.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] Other aspects and advantages of the present invention may become apparent upon reading the following detailed description and upon reference to the drawings in which:

[0025] **FIG. 1** shows a general diagram of wireless communications systems for which the key conversion system according to the principles of the present invention can be used;

[0026] **FIG. 2** is a block diagram illustrating the basic components of the prior art 2G global system for mobiles (GSM) network and security messages transmitted in the 2G GSM network;

[0027] **FIG. 3** is a block diagram illustrating the basic components of the prior art 3G UMTS network and messages transmitted in the 3G UMTS network;

[0028] **FIG. 4** is a block diagram illustrating the basic components of the prior art 2G IS-41 network and messages transmitted in the prior art 2G IS-41 network;

[0029] **FIG. 5** is a block diagram illustrating how a user roams from a 2G TDMA network into a generic 3G network;

[0030] **FIG. 6** is a block diagram illustrating how a user roams from a generic 3G network into a 2G TDMA network;

[0031] **FIG. 7** is a block diagram illustrating how a user roams from a 2G CDMA network into a generic 3G network;

[0032] **FIG. 8** is a block diagram illustrating how a user roams from a generic 3G network into a 2G CDMA network;

[0033] **FIG. 9** is a block diagram illustrating how a user roams from a 2G GSM network into a generic 3G network;

[0034] **FIG. 10** is a block diagram illustrating how a user roams from a generic 3G network into a 2G GSM network;

[0035] **FIG. 11** is a flow diagram of an embodiment of the forward conversion for the key conversion system according to principles of the present invention; and

[0036] FIG. 12 is a flow diagram of an embodiment of the reverse conversion for the key conversion system according to principles of the present invention.

DETAILED DESCRIPTION

[0037] An illustrative embodiment of the key conversion system according to the principles of the present invention is described below which provides an improved key conversion for a wireless unit which roams between first and second wireless communications systems. The key conversion system deterministically and reversibly converts an m bit key value of a first communications system into an n-bit key value of a second communication system. In certain embodiments, the key conversion system use three random functions f, g and h where random functions f and g map an m bit input string into an n-m bit string resembling a random number, and the random function h maps an n-m bit string into an m bit string resembling a random number. A random function maps inputs to outputs such that the outputs are unpredictable and random looking given the input. In the embodiments described below, the random functions are random oracles where every time an input is given it maps to the same output. Additionally, in the embodiments described below, the random functions are publicly known. For example, the random functions are known by the wireless communications system(s) involved in the intersystem handoff and the wireless unit.

[0038] The key conversion system is deterministic in that, given an m-bit key value, a wireless unit and the wireless communications system will determine the same n-bit key value without requiring an exchange of information. The key conversion system is reversible or bi-directional in that, if the wireless unit is handed off back to the first communications system, the n bit key of the second communications system is converted back to the m-bit key of the first communications system. The key conversion system provides improved security because even if almost all of the n bit key value is known, the m bit key value cannot easily be recovered. Similarly, if almost all of the m bit key value is known, the n bit key value is not easily recovered.

[0039] Depending on the embodiment, the key conversion system can provide secure, deterministic and bi-directional key conversion when a wireless unit roams between two wireless communications system, such as between an older communications system and a newer communications system. For example where the same reference numerals indicate like components, the IS-41 3G security scheme of FIG. 5 converts, at the VLR 80 and at the wireless unit 120 (or 122), the 520-bits VPM in combination with the 64-bits SMEKEY received from the VLR 110 to the 128-bit CK and/or 128-bit IK when the wireless unit roams into the 3G system from the 2G TDMA system. Conversely, as shown in FIG. 6, the IS-41 3G security scheme converts, at the VLR 80 and the wireless unit 90 (or 92), the 128-bit CK and/or the 128-bit IK to the 520-bits VPM in combination with the 64-bits SMEKEY when the wireless unit roams into the 2G TDMA system from the 3G system. The VLR 80 provides the VPM and the SMEKEY to the VLR 110.

[0040] As shown in FIG. 7, IS-41 3G security scheme converts, at the VLR 80 and at the wireless unit 120 (or 122), the 42-bits PLCM in combination with the 64-bits SMEKEY received from the VLR 110 to the 128-bit CK and/or the

128-bit IK when the wireless unit roams into the 3G system from the 2G CDMA system. Conversely, as shown in FIG. 8, the IS-41 3G security scheme converts, at the VLR 80 and at the wireless unit 90 (or 92), the 128-bit CK and 128-bit IK to the 42-bits PLCM in combination with the 64-bits SMEKEY when the mobile roams into the 2G CDMA system from the 3G system. The VLR 80 provides the PLCM and the SMEKEY to the VLR 110.

[0041] As shown in FIG. 9, the UMTS 3G security scheme converts, at the VLR 80 and at the wireless unit 60 (or 62), the 64-bit Kc received from the VLR 50 to the 128-bit CK and/or the 128-bit IK when the wireless unit roams into the 3G UMTS system from the 2G GSM system. Conversely, as shown in FIG. 10, the UMTS 3G security system converts, at the VLR 80 and at the wireless unit 90 (or 92), the 128-bit CK and/or the 128-bit IK to the 64-bit Kc when the wireless unit roams into the 2G GSM system from the 3G UMTS system. The VLR 80 provides the Kc to the VLR 50.

[0042] Accordingly, in certain embodiments, a wireless unit that supports enhanced subscriber authentication (ESA) and enhanced subscriber privacy (ESP) in a first communications system, such as a newer 3G communications system, may implement multiple privacy modes to enable the wireless unit to provide privacy using older algorithms in a second communications system, such as an older 2G TDMA communications system. Such a wireless unit can provide other forms of privacy after intersystem handoff to an MSC for an older second communications system that does not support ESP. When handoff to the older second communications system is required, the key conversion system can convert the key values for the newer first communications system to the privacy keys needed for the older privacy algorithms supported by the older second communications system. The keys for the second communications system can be sent to the target MSC of the second communications system from the MSC of the first communications system. Since the key conversion system is deterministic, the wireless unit will also have the keys for the second communications system by performing the same conversion as the first communication system using the key conversion system of the present invention.

[0043] The key conversion system maps a key(s) from a first system into a key(s) of a second system and back again. For example, when performing an intersystem handoff between a 3G communications system and a 2G TDMA system, the key conversion system can map a cipher key CK into a VPMASK/SMEKEY (VS) pair. In this embodiment, the key conversion function possesses the following properties: 1) A 128 bit CK is mapped into a 584 bit VS; 2) The function is reversible and maps back a 584 bit VS into a 128 bit CK; and 3) The function is secure in the sense that partial knowledge of the 584 bit key will not allow the adversary to recover the CK, nor will partial knowledge of 128 bit key CK allow the adversary to recover the 584 bit VS. In certain instances, for example when the call originates in a first communication system having a larger key value than the target second communications system, the conversion system maps the key value of the first communication system to a key value of a second communications system. However, if the wireless unit returns to the first communications system, the key conversion system maps the second key value to a subsequent key value for the first communications

system which is not necessarily the same as the original key value. Subsequent handoffs back to the first communications system from the second communications system produce a key value which is the same as the subsequent key value.

[0044] For example, when performing an intersystem handoff for a call originating with a 2G TDMA system to a 3G system, the key conversion system can map VPMASK/SMEKEY (VS) pair into a cipher key CK. In this embodiment, the key conversion function maps the 584 bit VS into the 128 bit CK. If the wireless unit is handed back to the 2G TDMA system, the conversion system maps back the 128 bit CK into the 584 bit VS, but the new 584 bit VS may not be the same as the original 584 bit VS. Subsequent handoffs to the 2G TDMA system from the 3G system will maintain the new 584 bit VS. Although this should not effect the security or operation of the wireless unit, the 128 bit CK is maintained the same all along in this embodiment.

[0045] In this embodiment, the key conversion system includes conversion functions available at the MSC in the newer system and at the wireless unit which will convert key values, for a first communications system, such as ESP keys, into key values of a second communications system, such as keys used for older privacy algorithms. In this example, the conversion function should convert the 128 bit CK key in the new first communication system to VPMASK/SMEKEY (VS) keys for the older second communication system. VPMASK is composed of 260 bits mask for each direction and SMEKEY is 64 bits long, for a total of 584 bits to be used by the older communication system. In case of an intersystem handoff from the old communication system to the new communication system, it may be useful for the conversion function to be reversible. The old communication system does not know about the new communication system and will transfer all 584 bits to the new communication system. The new communication system upon receiving the 584 bit key will realize that it needs to recover the 128 bit CK, and hence will compute the CK from the 584 bit key.

[0046] The VS keys created at the wireless unit and the MSC should be the same. This means the calculation of the VS keys must be based solely on CK and any other quantities known by both the MSC and the wireless unit. Otherwise, any new quantities (e.g. random number) would have to be exchanged between the wireless unit and the MSC prior to the conversion. The key conversion system does not require the exchange of information between the wireless unit and the new MSC and deterministically maps a CK to VS keys and VS keys to a CK key.

[0047] Additionally, weaknesses in the old communications system should not make the new communications system weak. One can achieve this by making the key conversion function cryptographically one way, so that even if the entire key of the old communication system, such as the VS key in this example, is revealed, the adversary cannot recover the key of the new communication system, such as the CK key in this example. However, this will make the system non-reversible and, as previously noted, the key conversion system should be reversible. Nevertheless, the key conversion system can be reversible and still provide almost all of the security of a non-reversible function. The security of the key conversion system in this example prevents an adversary from recovering any part of the CK

key even if almost all of the VS key is revealed except a small part. The adversary can guess the small part, but he should not be able to do any better. This aspect is important because parts of VPMASK may be somewhat easy to recover, and the entire VPMASK may be easier to recover than the SMEKEY. Yet if some part of the old system is hard to recover than the adversary will not know anything about CK. A similar security can apply to CK so that a partial knowledge of CK should not tell the adversary anything about VS.

[0048] In certain embodiments, the conversion function has two modes, the forward conversion and the reverse conversion. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the forward conversion takes the 128 bit randomly created CK key and expands it to 584 bit VS key. The reverse conversion function takes the 584 bit VS keys and maps it to a 128 bit CK key. In this embodiment, the forward conversion function is composed of 3 random functions f, g and h which map a given input into a random output. In this embodiment, these are not secret functions but public random functions known to everybody, including the adversary. These public random functions are referred to as random oracles in the literature. These random oracles can be implemented using hash functions and block ciphers as described below. In this example, the three random functions are f, g, h where f and g map a 128 bit input into a 456 bit random value, and h maps a 456 bit input into a 128 bit random value.

[0049] FIG. 11 shows a flow diagram of an embodiment of the forward conversion of the key conversion system for converting an m-bit key value KEY1 of a first communications system into an n-bit key value KEY2 of a second communications system. The m bit KEY1 is provided to a random function f (block 200) which maps an m-bit string into an n-m bit random number or first intermediate value R. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the conversion system converts a 128 bit key CK into a 584 bit key (VPMASK, SMEKEY). The 128 bit key CK is provided to the random function f (200) which maps the 128 bit CK into a 456 bit random number or first intermediate value R. The intermediate value R is provided to a random function h (block 210) which maps an n-m bit string into an m bit random number. The m-bit output of the function h (210) is subject to an exclusive-or (XOR 220) with the m bit KEY1 to produce an m-bit second intermediate value T. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the 456 bit intermediate value R is provided to the function h (210). The function h (210) maps the 456 bit value R to a 128 bit random number which is XORed with the 128 bit CK to produce a 128 bit second intermediate value T.

[0050] In the embodiment of FIG. 11, the m-bit intermediate value T is provided to a random function g (block 230). The random function g (block 230) maps an m bit string to an n-m bit random number which is subject to an exclusive-or (XOR 240) with the n-m bit intermediate value R to produce an n-m bit key value V which can be used as a key, keys or portion(s) of key(s). In this embodiment, the value V is a portion of the value KEY2 which can be used as a key, keys or portion(s) of key(s). In this embodiment, the n bit key KEY2 includes the n-m bit value V along with the m bit

second intermediate value T. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the random function g (230) maps the 128 bit intermediate value T into a 456 bit random number which is subject to the exclusive-or (XOR 240) with the 456 bit intermediate value T to produce the 456 bit key value V. The 456 bit value V and the 128 bit intermediate value T form the 584 bit key value KEY2 which in this example can be divided into the VPMASK and the SMEKEY for 2G TDMA systems.

[0051] The forward conversion of the CK of the 3G system to the VPMASK and SMEKEY of the 2G TDMA system can be written according to the following steps.

- [0052] 1. R=f(CK)/* create a 456 bit value from 128 bit CK by applying f */
- [0053] 2. T=h(R) XOR CK/* create a 128 bit value using h */
- [0054] 3. V=g(T) XOR R/* create a 456 bit value using g */
- [0055] 4. Output T,V/* output the 584 bit value */

[0056] FIG. 12 shows a flow diagram of an embodiment of the reverse conversion of the key conversion system for converting the n-bit key value KEY2 of the second communications system back into the m-bit key value KEY1 of the first communications system. In this embodiment, the n bit key value KEY2 is divided into an n-m bit first portion or value V and an m-bit second portion or value T. The m-bit value T is provided to the random function g (block 250) which maps an m-bit string into an n-m bit random number. The n-m bit random number is subjected to an exclusive-or (XOR 260) with the n-m bit key value V to produce the n-m bit first intermediate value R. In the example where the wireless unit roams back to the 2G TDMA system from the 3G system, the conversion system converts the 584 bit key (VPMASK, SMEKEY) into a 128 bit key CK. The 128 bit key value portion T is provided to the random function g (250) which maps the 128 bit T into a 456 bit random number. The 456 bit random number exclusive-ORED (XOR 260) with the 456 bit key value V to produce the 456 bit first intermediate value R.

[0057] In the embodiment of FIG. 12, the n-m bit first intermediate value R is provided to a random function h (block 270). The random function h (block 270) maps an n-m bit string to an m bit random number which is subject to an exclusive-or (XOR 280) with the m bit key value T to produce an m bit key value KEY1 which can be used as a key, keys or portion(s) of key(s). In the example where the wireless unit roams back to the 2G TDMA system from the 3G system, the random function h (270) maps the 456 bit intermediate value R into a 128 bit random number which is subject to an exclusive-or (XOR 280) with the 128 bit key value T to produce the 128 bit key CK.

[0058] The reverse conversion of the VPMASK and SMEKEY of the 2G TDMA system to the CK of the 3G system can be written according to the following steps.

- [0059] 1. Set T,V to 584 bit input/* T is 128 bit part, V is 456 bit part */
- [0060] 2. R=g(T) XOR V/* create 456 bit value R using T, V */
- [0061] 3. CK =h(R) XOR T

[0062] The random functions f, g and h can be implemented using hash functions and/or block ciphers. To implement the random functions f, g, and h, which can be referred to as random oracles, cryptographic hash functions, such as the functions known as known as SHA-1, MD5, RIPE-MD, can be used to instantiate the random functions f, g, h. A hash function can be typically characterized as a function which maps inputs of one length to outputs of another, and given an output, it is not feasible to determine the input that will map to the given output. Moreover, it is not feasible to find two inputs which will map to the same output. In using a SHA-1 hash function, each call to the SHA-1 hash function has a 160 bit initial vector (IV) and takes a 512 bit input or payload which is mapped into a 160 bit output. The IV is set to the IV defined in the standard for SHA-1 hash function. The payload will contain various input arguments: SHA(Type, Count, Input, Pad) where Type is a byte value which defines the various functions f, g, h. Function f and g will call SHA multiple times, and Count is a byte value which differentiates the multiple calls. Input is the input argument to the functions f, g, or h. Pad is zeroes to fill the remaining bit positions in the 512 bit SHA payload. Below is an example procedure for implementing the random function f, g and h using a hash function routine referred to as SHA.

- [0063] SHA(type,count,input,Pad)
- [0064] f(CK): SHA(1, 1, CK, pad)
- [0065] SHA(1, 2, CK, pad)
- [0066] SHA(1, 3, CK, pad) mod 2^{136}
- [0067] h(R): SHA(2, 1, R, pad) mod 2^{128}
- [0068] g(T): SHA(3, 1, T, pad)
- [0069] SHA(3, 2, T, pad)
- [0070] SHA(3, 3, T, pad) mod 2^{136}
- [0071] Block ciphers, like AES, can be used to create functions f, g, and h.
- [0072] f(CK): $E_{CK}(1); E_{CK}(2); E_{CK}(3); E_{CK}(4) \bmod 2^{72};$
- [0073] h(R): $E_{K0}(R1 \bmod 5) \bmod E_{K0}(R2 \bmod 6) \bmod E_{K0}(R3 \bmod 7) \bmod E_{K0}(R4 \bmod 8)$
- [0074] g(T): $E_T(9); E_T(10); E_T(11); E_T(12) \bmod 2^{72};$
- [0075] where in f(CK), CK is used as the key in the block cipher and 512 bit stream is produced by encrypting 1 . . . 4 in counter mode. The last encryption is truncated from 128 bit to 72 bit to get the needed 456 bits. In h(R), a public key K0 is used to encrypt the parts of 456 bit R and the resulting ciphertexts are exclusive-ored together. R1, R2, and R3 are 128 bit values and R4 is the remaining 72 bit value of R, padded with zeroes to complete 128 bits.

[0076] Thus, the key conversion system provides bi-directional, deterministic and secure conversion of a key(s) or portion(s) thereof between first and second communications systems. The key conversion system is secure in the forward direction in that given most of the output KEY2 (for example, T,V), an adversary cannot recover KEY1 (for example, CK). In the example with the 2G TDMA and 3G systems, if all of T and most V except say 64 bits are known, then parts of R can be recovered, but not all of R by

calculating $R=g(T) \text{ XOR } V$. An attempt can be made to recover some of CK by performing $CK=h(R) \text{ XOR } T$. However, since all of R is not known, even a bit of information about $h(R)$ cannot be recovered, assuming h is a random function. Hence no information can be recovered about CK. Similarly, if all of V and part of T are known, except say 64 bits of T, then no information about CK can be recovered. Since we do not know all of T, the intermediate value R cannot be calculated using $g(T) \text{ XOR } V$. Thus without the intermediate value R, no progress can be made in recovering any information about CK.

[0077] Similarly, the key conversion system is secure in the reverse direction in that given most of the output KEY1 (for example, CK), an adversary cannot recover KEY2 (for example, T, V). In the example with the 2G TDMA and 3G systems, if a part of CK is known, no information about T, V can be recovered. Since we do not know all of CK, the intermediate value R cannot be calculated using $f(CK)$. Thus without the intermediate value R, no progress can be made in recovering any information about T, V.

[0078] In addition to the embodiment(s) described above, the key conversion system according to the principles of the present invention can be used which omit and/or add input parameters and/or random functions or other operations and/or use variations or portions of the described system. For example, the key conversion system has been described as converting between n bit key of a first communication system and an m bit key of a second communications system using random oracles f, g and h where the random oracles f and g map an m bit string to a n-m bit random number and the random oracle h maps a n-m bit string to an m bit random number. However, different random functions can be used as well as different or additional functions which map x bit strings to y bit random numbers and/or map y bit strings to x bit random numbers where x or y can be equal to n-m or m. Additionally, the m bit key value for the first communications system can be a key, keys or portion(s) thereof, and the n bit key value for the second communications system can be a key, keys or portion(s) thereof. For example, the example with the 2G TDMA and 3G systems, the conversion is between the 128 bit CK of the 3G system and the 584 bit key value for the SMEKEY and VPMASK of the 2G TDMA system, but the conversion could be between a 256 bit key value of CK and IK of the 3G system and the 584 bit key value for the SMEKEY and VPMASK of the 2G TDMA system.

[0079] In the example described above, a forward conversion is from the m bit key value of the first communications system to the n bit key value of the second communications system where the first communications system corresponds to the new system and the second communications corresponds to the old system and where $m < n$. However, depending on the embodiment, the first communications system can be older, and the second communications system is newer. Alternatively, the forward conversion can be the conversion of the smaller size key value of one communications system to the larger bit size key value of another communications system, and the reverse conversion is the conversion of the larger bit size key value to the smaller size key value. Depending on the embodiment, the conversion of different, larger, smaller and/or the same size(s) of key value(s) between the different communications systems are possible.

[0080] Furthermore, the key conversion system can be used to handle the intersystem handoffs described in the FIGS. 5-10 to convert a key, keys or portion(s) thereof from one communications system to the key, keys or portion(s) thereof of another communications system. It should be understood that different notations, references and characterizations of the various values, inputs and architecture blocks can be used. For example, the functionality described for the key conversion system can be performed in a home authentication center, home location register (HLR), a home MSC, a visiting authentication center, a visitor location register (VLR) and/or in a visiting MSC. Moreover, the key conversion system and portions thereof can be performed in a wireless unit, a base station, base station controller, MSC, VLR, HLR or other sub-system of the first and/or second communications system. It should be understood that the system and portions thereof and of the described architecture can be implemented in or integrated with processing circuitry in the unit or at different locations of the communications system, or in application specific integrated circuits, software-driven processing circuitry, programmable logic devices, firmware, hardware or other arrangements of discrete components as would be understood by one of ordinary skill in the art with the benefit of this disclosure. What has been described is merely illustrative of the application of the principles of the present invention. Those skilled in the art will readily recognize that these and various other modifications, arrangements and methods can be made to the present invention without strictly following the exemplary applications illustrated and described herein and without departing from the spirit and scope of the present invention.

1. A method of converting a first key value for a first communications system to a second key value of a second communications, said method comprising:

generating a first intermediate value from at least a portion of said first key value using a first random function;

providing at least a portion of said first intermediate value to a second random function to produce a second value;

performing an exclusive-or on at least a portion of said first key value and at least a portion of said second value to generate a second intermediate value;

providing at least a portion of said second intermediate value to a third random function to produce a third value; and

producing at least a first portion of said second key value by performing an exclusive-or on at least a portion of said third value and at least a portion of said first intermediate value.

2. The method of claim 1 comprising:

producing at least a portion of said second intermediate value as at least a second portion of said second key value.

3. The method of claim 1 wherein said generating comprises the step of:

providing said first key value of m bits to a first random function to produce said first intermediate value of n-m bits.

4. The method of claim 3 wherein said first steps of providing and performing comprise:

providing said n-m bit first intermediate value to a second random function to produce an m bit second value; and performing an exclusive-or on said m bit first key value and said m bit second value to generate said second intermediate value with m bits.

5. The method of claim 4 wherein said second step of providing and said step of producing comprise:

providing said m bit second intermediate value to a third random function to produce a n-m bit third value; and performing an exclusive-or on said n-m bit third value and said n-m bit first intermediate value to generate an n-m bit portion of said second key value.

6. The method of claim 5 comprising:

providing said m bit second intermediate value as an m bit second portion of said second key value having n bits.

7. The method of claim 2 further comprising the steps of:

providing said second portion of said second key value to said third random function to produce said third value; and

generating said first intermediate value by subjecting said first portion of said second key value to an exclusive-or with said third value.

8. The method of claim 7 further comprises:

using said second random function to generate said second value from said first intermediate value; and

producing at least a portion of said first key by subjecting said second value to an exclusive-or with said second portion of said second key value.

9. The method of claim 6 further comprises:

providing said m bit first portion of said n bit second key value to said third random function to produce said n-m bit third value; and

generating said n-m bit first intermediate value using an exclusive-or of said n-m bit second portion of said n bit second key value with said n-m bit third value.

10. The method of claim 9 further comprises:

providing said n-m first intermediate value to said second random function to generate an m bit second value; and

producing said portion of said first key value having m bits by using an exclusive-or of said m bit first portion of said second key value with said m bit second value.

11. A key conversion system for converting a first key value for a first communications system to a second key value of a second communications, said system comprising:

processing circuitry adapted to generate a first intermediate value from at least a portion of said first key value using a first random function to provide at least a portion of said first intermediate value to a second random function to produce a second value, to perform an exclusive-or on at least a portion of said first key value and at least a portion of said second value to generate a second intermediate value, to provide at least

a portion of said second intermediate value to a third random function to produce a third value and to produce at least a first portion of said second key value by subjecting at least a portion of said third value to an exclusive-or with at least a portion of said first intermediate value.

12. The system of claim 11 wherein said processing circuitry further configured to produce at least a portion of said second intermediate value as at least a second portion of said second key value.

13. The system of claim 12 wherein said processing circuitry further configured to provide said first key value of m bits to a first random function to produce said first intermediate value of n-m bits.

14. The system of claim 13 wherein said processing circuitry further configured to provide said n-m bit first intermediate value to a second random function to produce an m bit second value and to perform an exclusive-or on said m bit first key value and said m bit second value to generate said second intermediate value with m bits.

15. The system of claim 14 wherein said processing circuitry configured to provide said m bit second intermediate value to a third random function to produce a n-m bit third value and to perform an exclusive-or on said n-m bit third value and said n-m bit first intermediate value to generate an n-m bit portion of said second key value.

16. The system of claim 15 wherein said processing circuitry configured to provide said m bit second intermediate value as an m bit second portion of said second key value having n bits.

17. The system of claim 12 wherein said processing circuitry configured to provide said second portion of said second key value to said third random function to produce said third value and to generate said first intermediate value by subjecting said first portion of said second key value to an exclusive-or with said third value.

18. The system of claim 17 wherein said processing circuitry configured to use said second random function to generate said second value from said first intermediate value and produce at least a portion of said first key by subjecting said second value to an exclusive-or with said second portion of said second key value.

19. The system of claim 16 wherein said processing circuitry configured to provide said m bit first portion of said n bit second key value to said third random function to produce said n-m bit third value and to generate said n-m bit first intermediate value using an exclusive-or of said n-m bit second portion of said n bit second key value with said n-m bit third value.

20. The system of claim 19 wherein said processing circuitry is configured to provide said n-m first intermediate value to said second random function to generate an m bit second value and to produce said portion of said first key value having m bits by using an exclusive-or of said m bit first portion of said second key value with said m bit second value.

* * * * *